

PrivacyTRACKER

iapp

A publication from the International Association of Privacy Professionals

Lame Ducks and Top Dogs: Privacy's Path in 2008 and the Coming Administration

Mike Spinney, CIPP

When the dust settled after the 2004 elections, the privacy community looked ahead at likely changes to the legal landscape in hopes of divining what new laws and legal developments might affect the profession and their individual situations. A growing number of states had either passed or were considering privacy laws in the mold of California's landmark breach notification legislation, SB 1386, and conventional wisdom held that the 109th Congress, in the face of an increasingly complex regulatory environment, would soon enact overarching federal law to provide a minimum

standard for all states to follow.

Similarly, the success of the national Do Not Call Registry seemed likely to spawn well-meaning copycat laws addressing junk mail, email, and other consumer annoyances. By all accounts, the next two years would be busy for legislators and privacy professionals.

It was not to be, however, as matters of foreign policy and economics took priority. Privacy bills such as the 2005 Leahy-Specter Personal Data Privacy

See Lame Ducks and Top Dogs, page 3

State Privacy and Data Protection Laws: Let's Recap

Alysa Zeltzer Hutnik

The year 2007 continued a trend of many states enacting a wide range of privacy and data protection laws in the absence of a uniform federal law on this front. This article provides an analysis of the key data breach notification laws and the myriad of other state laws enacted to date that regulate how businesses handle personal information.

I. State Data Breach Notification Laws

The patchwork of state data breach notification laws steadily increased in 2007. To date, 38 states and the District of Columbia have enacted laws that require businesses to comply

with notification obligations upon the discovery of a suspected data breach¹. In short, these laws require businesses to (1) assess whether a potential data compromise qualifies as a "security breach" based on the type of personal data involved and the extent of the compromise, and (2) issue one or more forms of notification within a

See Privacy and Protection Laws, page 4

In This Issue

Lame Ducks and Top Dogs: Privacy's Path in 2008 and the Coming Administration..... 1

State Privacy and Data Protection Laws: Let's Recap..... 1

Letter from the Editor..... 2

Legislative Action..... 7

Credit Agencies & ID Theft..... 7

Data Security & Breach..... 19

Government Records, SSN & Identification..... 25

Internet..... 40

Marketing..... 43

Children & Education..... 51

Financial, Insurance & Mortgages..... 56

Employment..... 62

Medical..... 63

Telecommunications & RFID..... 68

Miscellaneous..... 71

Session Calendar 2008..... 72



regulations, the FTC is often used as a barometer to determine just how seriously the government takes the rules they put on the books.

Jessica Rich, assistant director of the FTC's Division of Privacy and Identity Protection said that the FTC is prohibited from offering specific forecasting on matters of policy or potential Congressional action, and cannot comment on matters of ongoing or probable enforcement action, but could offer some insight as to what issues will receive attention from the Commission.

Rich observed that "privacy is no longer on the front burner in Washington," but that certain areas of interest to the privacy community would be considered throughout the coming year.

Specifically, Rich said that behavioral targeting was on the agenda, as the FTC seeks to help the industry by providing guidelines for self-regulation. At this writing, the FTC is still in the process of collecting public comment on its proposed guidelines, and has extended the period of public comment to April 11 from February 22. The FTC has also fielded requests for hearing in Congress on the subject as lawmakers seek to inform themselves on behavioral targeting's potential impact on consumers.

The FTC, as part of a seventeen agency presidential task force on identity theft, is also in the process of developing a report on possible reforms aimed at protecting Social Security numbers. Efforts within government and private industry to reduce reliance on SSNs as an element of identification have been encouraging, but there remains a long way to go as some agencies, such as Medicare, still use SSNs.

Rich also said that data protection would continue to receive the Commission's attention. Pointing to recent enforcements of Disposal Rule violations and the settlement of a complaint against clothing retailer Life is Good for failure to provide adequate and promised safeguarding of customer data, including credit card information, Rich said that protecting consumer information "will continue to be a huge area for FTC action."

The FTC will also be working with the U.S. Department of Commerce on the development of a global framework for privacy within the various management regimes among Asia-Pacific (APAC) nations. The goal of the framework will be to allow for data sharing between countries under a reciprocal agreement to provide enforcement, ensuring that cross-border transactions, including data sharing, among APAC trading partners can continue without hampering trade.

The difficulty will be in reconciling the privacy standards of APAC countries with relatively mature bodies of privacy law, such as the U.S., with countries whose engagement in privacy are just getting underway.

"Managing privacy [across borders] is an enormous challenge, and something we'll be working on," Rich said, explaining that the Commerce Department will have the lead on the effort, but that the FTC, as the U.S.'s enforcement body, will play a major role in developing the program.

So while there are plenty of bell cows to help the privacy community discern where the trends are leading, it's anyone's guess as to what major developments—if any—to expect in privacy's near future. After all, lame ducks sometimes become the goose that lays the golden egg.

Mike Spinney, CIPP, is principal of SixWeight, a communications consultancy in Townsend, Massachusetts providing strategic, privacy-savvy advice to companies in the information marketplace. Spinney is a member of the Ponemon Institute, co-chair of the Boston KnowledgeNet chapter, and a regular contributor to IAPP newsletters. He can be contacted at 978-597-0342, or mike@sixweight.com.

Privacy and Protection Laws

continued from page 1

relatively short period of time.

A. Assessing If and How the Breach Notification Laws Apply

In most states, notice is only required if the potential data compromise involves computerized personal data. Only five states—Hawaii, Indiana, Maryland, North Carolina, and Wisconsin—also extend their breach notification laws to personal data stored in hard copy format. In addition, most breach notification laws are triggered only if the potentially compromised information includes very sensitive personal information, such as consumer names with Social Security numbers or financial account numbers with pin or pass codes. But a few state breach notification laws are more expansive and require notice if the breach involves financial account numbers without a pin or pass code, health information, birth date, mother's maiden name, or a government-issued or employee identification number.

Also, when determining which state laws are triggered, one must identify which states the compromised consumer data implicates based on the affected consumers' residence. But four states—Arizona, Hawaii, New

Hampshire, and Oregon—expand that analysis by not limiting their notification requirement to residents of the home state.

Finally, notice is not required in any of the breach notification states if the personal information is encrypted and the keys to unlock the encryption were not also compromised. A good number of the states also provide the business with some discretion not to issue notice if the breach is not likely to result in harm to consumers. Determining the extent of such discretion, however, requires a careful parsing of the particular state laws that are implicated in a given breach as the statutory language varies considerably from state to state.

B. Fulfilling the Notification Obligations

If notice to consumers is required under the data breach notification laws, then the business must promptly deliver notice to the affected consumers. Most of the states do not set a specific timetable for delivering such notice, but typically require that notice be provided as soon as is reasonably practicable or in the most expedient time possible. Three states—Florida, Ohio, and Wisconsin—require that the notice be provided within 45 days after discovering the breach.

For the method of notice, most states provide businesses with a choice of how to deliver notice, typically either in writing, electronically, or by telephone. For the notice content, eleven states specify what exactly must be in the notice: Hawaii, Maryland, Michigan, New Hampshire, New

York, North Carolina, New York, North Carolina, Oregon, Vermont, and Wyoming. Under these laws, as well as those that do not specify the type of content, the notice typically must include a general description of the breach, the approximate date of the breach, the type of personal information obtained as a result of the breach, the contact information of the company and the national consumer reporting agencies, and advice to the consumer to report suspected identity theft to law enforcement.

Depending on the states implicated, the company also may need to send notice to state regulators and credit reporting agencies (CRAs). For regulator notice, nine states require that notice of the breach be sent to specified law enforcement agencies. Specifically, Delaware, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, and New York require such regulator notice regardless of how many consumers were affected by the breach (although in New Jersey and Maryland, the regulator notice must be sent before the consumer notice). In Hawaii and North Carolina, regulator notice is required only if there are more than 1,000 affected consumers. Under Vermont's law, notification to the Vermont Attorney General must be provided only if an investigation reveals that misuse of breached personal information is not reasonably possible.

For CRA notice, 22 states and the District of Columbia require businesses to notify CRAs upon learning of a breach (but, in most states, only if certain thresholds are met). For example, Indiana has no numerical thresh-

old for notification of CRAs, while in Minnesota, the threshold is 500 consumers. In Colorado, Delaware, the District of Columbia, Florida, Hawaii, Kansas, Maine, Maryland, Michigan, Nevada, New Hampshire, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, Tennessee, and Vermont, notice must be provided to CRAs if more than 1,000 consumers are notified. In New York, the threshold is 5,000, and Georgia and Texas have a threshold of 10,000. Montana requires CRA notice only if the notice to consumers mentions credit reports.

Finally, all of the statutes require a third party that maintains personal information on behalf of another business to notify that business if a breach occurs so that the business can deliver the required notice.

II. Information Safeguard Laws

Given that data breach notification only applies after-the-fact, a number of states have enacted broader forms of information safeguard laws—either regulating information handling in general, or certain types of information. For example, nine states—Arkansas, California, Maryland, Nevada, North Carolina, Oregon, Rhode Island, Texas, and Utah—have enacted laws requiring businesses to implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use, modification, or disclosure. The scope of these laws is typically limited to businesses that own or license information about a customer residing in the state.

There are, however, some vari-

¹ Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Vermont, Washington, Wisconsin, and Wyoming.

ances among these laws. The Oregon safeguard law identifies specific administrative, technical, and physical safeguards as examples of the measures necessary to demonstrate compliance with the law. The Texas safeguard law further specifies that the obligation to implement and maintain reasonable safeguard procedures includes taking any appropriate corrective action. The Nevada law also expressly requires businesses to encrypt certain personal information if transferring that information electronically outside of the secure business network. The California law also prohibits businesses from recording personal information on transaction records. And about half of the laws expressly require that when businesses share or provide access to personal data to third parties, they must require the third parties to protect the personal information to the same extent that the business must protect that information, by contract. Finally, the North Carolina law is limited to licensed insurers, and the Oregon, Texas, and Utah safeguard laws contain an exemption for financial institutions.

In addition to the information safeguard laws, 19 states regulate how businesses must dispose of records containing personal data. The disposal laws in Arkansas, California, Georgia, Hawaii, Indiana, Kentucky, Maryland, Massachusetts, Michigan (health care providers only), Montana, Nevada, New York, Oregon, Tennessee, Texas, Utah, Vermont, Washington, and Wisconsin (financial institutions, medical businesses, and tax preparation

businesses only) require that, when a business disposes of customer records containing personal information, the business must destroy the records by shredding, erasing, or otherwise modifying the records to make them unreadable² or undecipherable. Civil penalties apply for violations.

In addition, 24 states have enacted laws requiring businesses to protect Social Security numbers from public access.³ These requirements typically prohibit businesses from making SSNs available to the general public online or offline, requiring consumers to transmit a SSN over the Internet unless the connection is secure or the number is encrypted, requiring consumers to log onto a Web site using a SSN without a password, printing SSNs on identification cards or badges, or printing SSNs on anything mailed to a consumer unless required by law or the document is a form or application. In New Jersey and New York, these requirements apply to even truncated SSNs. Further, the New Mexico SSN law expressly requires businesses to also implement policies that limit access to SSNs to authorized employees and to hold such employees responsible for unauthorized release of SSNs. None of these laws, however, prohibit businesses from using SSNs for internal verification or other administrative purposes so long as they have reasonable procedures in place to protect the confidentiality and security of the personal data.

Finally, one state—Minnesota—has created an added incentive for businesses

to better protect financial cardholder data against compromise by creating financial liability for the business after a data breach. The law prohibits businesses from retaining the card security code data, the pin verification code number, or any magnetic stripe data after the transaction's authorization. If businesses violate these requirements, they may be required to reimburse banks for the cost of reasonable actions undertaken to respond to a breach, including the costs of canceling and reissuing credit and debit cards, closing or reopening accounts, stop-payment actions, unauthorized transaction reimbursements, and the providing of breach notification to account holders.

Several states have similar legislation pending and, given the ever-increasing focus on privacy, we are likely to see a growing number of these and other privacy and/or data protection laws enacted in 2008.

Alysa Hutnik is an attorney in the Advertising, Privacy, and Information Security practice of Kelley Drye & Warren LLP in Washington, D.C. She counsels clients on compliance with federal and state consumer protection and privacy and information security laws. She is also the Chair of the forthcoming American Bar Association Handbook on Data Security (a practical guide for in-house practitioners). She can be reached at ahutnik@kelleydrye.com.

² Some of these disposal laws exempt certain industries that already are heavily regulated by federal or state law. For example, financial institutions are exempt from the state disposal laws in Hawaii, Texas, Utah, and Vermont, and insurers and credit reporting agencies are exempt under the Hawaii, Texas, and Vermont disposal laws.

³ Arizona, Arkansas, California, Colorado, Connecticut, Georgia, Hawaii, Illinois, Maryland, Massachusetts, Michigan, Minnesota, New Jersey, New Mexico, New York, North Carolina, Oklahoma (employers only), Oregon, Pennsylvania, Rhode Island, Texas, Utah (insurers only), Vermont, and Virginia.

Legislative Action

The following bills were active during the period between February 1-27, 2008. The most recent activity on each bill is provided.

Credit Agencies & Identity Theft

AK H 65	<p>TITLE: Personal Information and Consumer Credit INTRODUCED: 01/16/2007 LOCATION: House Rules Committee SUMMARY: Relates to breaches of security involving personal information, credit report and credit score security freezes, consumer credit monitoring, credit accuracy, protection of social security numbers, care of records, disposal of records, identity theft, furnishing consumer credit header information, credit cards, and debit cards, and to the jurisdiction of the office of administrative hearings; amends Rule 60, Alaska Rules of Civil Procedure.</p> <p>STATUS: 02/21/2008 From HOUSE Committee on FINANCE: Without recommendation with substitute. 02/21/2008 To HOUSE Committee on RULES.</p>
AL H 404	<p>TITLE: Consumer Reports INTRODUCED: 02/12/2008 LOCATION: House Banking and Insurance Committee SUMMARY: Provides procedures for placing security freezes on consumer reports; requires a consumer reporting agency to put a security freeze on a consumer report upon request of a consumer; provides a procedure to temporarily lift or remove a security freeze on a report; provides for payment of a fee by the consumer; creates a cause of action for damages incurred as a result of a reporting agency's failure to place a security freeze on a consumer's credit report.</p> <p>STATUS: 02/12/2008 INTRODUCED. 02/12/2008 To HOUSE Committee on BANKING AND INSURANCE.</p>
AZ H 2587	<p>TITLE: Extension of Credit in Identity Theft INTRODUCED: 01/18/2008 LOCATION: Senate Financial Institutions, Insurance and Retirement Committee SUMMARY: Relates to consumer reporting agencies and fair credit reporting; relates to requiring certain practices by credit card issuers to prevent identity theft and fraudulent application for credit cards.</p> <p>STATUS: 02/26/2008 To SENATE Committee on FINANCIAL INSTITUTIONS, INSURANCE AND RETIREMENT. 02/26/2008 Additionally referred to SENATE Committee on RULES.</p>
AZ H 2604	<p>TITLE: Consumer Reports INTRODUCED: 01/18/2008 LOCATION: House Commerce Committee SUMMARY: Concerns consumer reports; relates to security freeze.</p> <p>STATUS: 02/21/2008 To HOUSE Committee on COMMERCE. 02/21/2008 Additionally referred to HOUSE Committee on RULES.</p>
AZ H 2707	<p>TITLE: Identifying Information Theft INTRODUCED: 01/31/2008 LOCATION: House Commerce Committee SUMMARY: Concerns identifying information; relates to theft; relates to penalties.</p> <p>STATUS: 02/05/2008 To HOUSE Committee on COMMERCE. 02/05/2008 Additionally referred to HOUSE Committee on RULES.</p>