ANDREWS LITIGATION REPORTER

THOMSON WEST

Privacy

COMMENTARY

REPRINTED FROM VOLUME 3, ISSUE 4 / DECEMBER 2005

To Notify or Not to Notify?

By Robin B. Campbell, Esq.*

Gone are the times when privacy compliance was only an issue for U.S. corporations with operations in Europe and a handful of other foreign jurisdictions. These days corporate privacy officers all over the United States are kept busy ensuring compliance with myriad state and federal laws falling within the privacy arena.

The Privacy Act, Health Insurance Portability and Accountability Act, Children's Online Privacy Protection Act, Gramm-Leach-Bliley Act, Fair Credit Reporting Act, the CAN-SPAM Act, state and federal laws on Social Security number usage, and more recently — with the California Legislature leading the way — state security breach laws all impose obligations on organizations to protect the personal information of individuals, including customers, employees and suppliers.

Given the increasing number of high-profile security breaches in 2005 and the heightened awareness that such breaches are occurring, many states have adopted legislation mandating notification to individuals whose personal information has bee :n compromised. As of September 21 states had enacted their own version of security-breach-notification laws and more were under consideration.

Some states have focused on protecting against identity theft and financial loss and, therefore, have established a materiality requirement or threshold of harm before notification is required. Others have taken this opportunity to promulgate some general privacy protections similar to those enacted in Europe and elsewhere. Still others have limited the application of this type of law to entities that are most likely to process large amounts of personal information, including data brokers and government entities.

Finally, some have elected to cover every type of person or entity without exclusion for those already under the jurisdiction of federal or state privacy regulations, such as Gramm-Leach-Bliley or HIPAA. The existence of at least 21 different statutes with inconsistent scope and detailed requirements obliges any entity handling personal information to look carefully at each state's laws to determine the best route to compliance.

The 21 states that currently have security-breach-notification laws on the books are Arkansas, California, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Maine, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Rhode Island, Tennessee, Texas and Washington. Such laws are under consideration in many other states.

The Benchmark

In advance of any breach, California Civil Code Section 1798.81.5 requires a business to implement and maintain reasonable security procedures and practices and to contractually require the same of any nonaffiliated third parties to whom personal information is transferred. California also requires businesses to utilize appropriate data-destruction methods when disposing of records containing personal information.

All of the newly enacted laws in various states use California's definition of personal information as a baseline, and some expand upon it. California's law defines personal information, for notification purposes, as an individual's first name or initial and last name in combination with one or more of the following when either the name or the data elements are not encrypted: Social Security number, driver's license number or California identification number, account number, or credit or debit number in combination with any required security code, access code or password that would permit access to an individual's financial account.

Under the security-breach law of California, any person or business that conducts business in the state must notify

residents "in the most expedient time possible and without unreasonable delay" if their computerized personal information was or is reasonably believed to have been acquired by an unauthorized person. The notice can be written or electronic.

If the cost of notice exceeds $250,000, if the affected class of persons exceeds 500,000, or if the person or business does not have sufficient contact information, substitute notice may be used. Substitute notice includes e-mail notice, conspicuous posting of the notice on a Web site or notification to major statewide media. The California Office of Privacy Protection recommends that notice be given in the form of a letter explaining what happened to the individual's information (*e.g.*, hacker broke into system or laptop was stolen) and offering advice on how to protect oneself from identity theft (*e.g.*, close credit card accounts, establish fraud alerts and review credit reports carefully).

Finally, under the California law, a person or business may use its own notification procedures as part of a data security policy for personal information if its procedures are consistent with the state law's timing requirements of expedient notification and if the person or business notifies individuals in accordance with its own policy in the event of a breach.

Using the California law as a benchmark, I summarize here the basic differences in the state legislation that has followed.

The State Laws

Arkansas SB 1167

Arkansas adds medical information to the list of data that constitutes personal information. The Arkansas law states that notification is not required if "after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers," which gives businesses an out if there is no real threat of identity theft.

Although Arkansas limits its security-breach law with respect to when notice is required, it expands the law when it comes to protecting personal information in advance of a breach. Arkansas requires businesses dealing with personal information to implement and maintain reasonable security procedures and practices and to employ appropriate methods of destroying personal information.

Arkansas also provides an exemption for persons or businesses subject to federal or state laws that provide greater protection for personal information or laws that have equally stringent disclosure requirements. Unlike California, Arkansas does not provide a private right of action and instead leaves enforcement to the attorney general.

Connecticut SB 650

Connecticut also provides a component for the likelihood of harm. Notification is not required if "after appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired or accessed."

Connecticut provides an exemption for entities already subject to security-breach regulation under Gramm-Leach-Bliley. Finally, the Connecticut statute specifically designates a violation of the security-breach-notification law as an unfair trade practice enforceable by the attorney general.

Delaware HB 116

The Delaware statute adds medical information to the list of data that constitute personal information. In addition to notifying the individuals affected, Delaware requires that the Department of Justice's Consumer Protection Division also be notified. The Delaware law also provides an exemption for entities already subject to state or federal laws providing greater protection to personal information.

Finally, the Delaware statute provides an individual right of action for a violation of its new law (in addition to attorney general enforcement), including recovery of treble damages and attorney fees.

Florida HB 481

Rather than utilizing the California time frame for notice, Florida sets a time frame of 45 days following determination of a breach. If the entity is licensing or otherwise does not own the data, it must notify the owner of the data within 10 days of the breach.

Florida also includes a threshold showing of materiality and does not require notice of a breach if, after reasonable investigation, it is determined that the breach "has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed." The Florida law also mandates notification to consumer reporting agencies when notifying more than 1,000 individuals of a breach.

Georgia SB 230

The Georgia law is limited in application to "information brokers." An "information broker" is defined as "any person or entity who, for monetary fees or dues, engages in

whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement or licensing purposes."

The Georgia law slightly modifies the definition of "personal information" to include any of the data elements not containing an individual's name, if the information compromised would be sufficient to allow identity theft. Georgia also requires notification to consumer reporting agencies in the event that more than 10,000 individuals are being notified of a breach.

Illinois HB 1633

The Illinois law basically follows the California statute and provides that a violation constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.

Indiana SB 503

Indiana has limited its security-breach law to state agencies. The law requires state agencies to notify consumer reporting agencies and individuals of a security breach if the number of individuals affected exceeds 1,000.

Louisiana SB 205

The Louisiana law does not require notification if, after investigation, it is determined that there is no reasonable likelihood of harm to customers. The Louisiana law also provides a private right of action to its residents. Under the new law, financial institutions governed by the federal interagency guidelines are deemed compliant. Louisiana also establishes a private right of action.

Maine LD 1671

Like Georgia, Maine has limited its security-breach-notification law to data brokers and includes in its definition of "personal information" data not containing an individual's name, if the information would be sufficient to allow identity theft.

If more than 1,000 residents are affected, a data broker must also notify consumer reporting agencies. Data brokers are also required to notify state regulators or the attorney general of a security breach.

Minnesota HF 2121

The Minnesota law closely tracks California's but provides an exemption for entities governed by Gramm-Leach-Bliley and HIPAA and requires notification to consumer reporting agencies if notice is provided to more than 500 people.

Montana HB 732

Montana expands California's definition of "personal information" to include: "an individual's name, signature or telephone number in combination with one or more additional pieces of information about the individual, consisting of the individual's passport number, driver's license number, passwords, or personal identification numbers required to obtain access to the individual's finances or any other financial information as provide by rule. A Social Security number in and of itself constitutes personal information."

Montana also requires that data be "materially compromised" before notification of a breach is required. The state mandates reasonable destruction methods for all personal information. Montana also has a special provision for licensees or insurance support organizations operating in the state. These entities are required to develop and maintain an information security policy for safeguarding personal information and security-breach-notice procedures that provide expedient notice to individuals.

Nevada SB 347

Nevada has a materiality threshold before notification of a security breach is required. However, the state has some of the most restrictive notice requirements in advance of a breach. Nevada, like most other states with pre-breach requirements, mandates appropriate data destruction procedures.

In addition Nevada requires reasonable security measures to protect personal information, a contractual provision requiring reasonable security measures when personal information is disclosed to a third party and the use of encryption for any electronic transfer (other than facsimile) of personal information. Although certain entities can be exempt from the first two requirements and entities subject to Gramm-Leach-Bliley are exempt from the general notification requirements, there are no exemptions given for the use of encryption for electronic transfers. If more than 1,000 notifications are involved, an entity must send notices to all consumer reporting agencies.

New Jersey A4001

The New Jersey law does not require notice in the event of a security breach if "the business or public entity establishes that misuse of the information is not reasonably possible." New Jersey also mandates appropriate destruction methods for personal information that make

it unreadable, undecipherable or incapable of reconstruction. If more than 1,000 people are notified of a security breach pursuant to the New Jersey law, all consumer reporting agencies must also be notified.

New York SB 5827

The New York law provides two definitions of information. "Personal information" is as any information concerning a natural person that, because of name, number, personal mark or other identifier, can be used to identify such natural person. New York sets out a second definition for "private information" that more closely mimics the California law such that "private information" comprises "personal information" combined with one or more of the following: Social Security number, driver's license number, ID card number, or account or credit/debit card number with access code or password.

A breach occurs when there is "unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality or integrity of personal information maintained by a business." The New York law also provides factors to consider when determining whether information has been acquired or is reasonably believed to have been acquired. These factors are:

- Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information;
- Indications that the information has been downloaded or copied; or
- Indications that the information was used by an unauthorized person, such as when fraudulent accounts are opened or instances of identity theft reported.

Notice, on the other hand, is required when there is a "breach of the security system" and any *private information* of a New York resident was or is reasonably believed to have been acquired by a person without valid authorization. New York provides the same means and timing for notice but also requires telephone notice, provided a log of each notification is kept.

Unlike California, New York does not provide a private right of action for individuals injured by a security breach. Instead, it gives the attorney general authority to sue for damages on behalf of individuals, including consequential financial losses. New York also adds civil penalties for any business that knowingly or recklessly violated its security-breach law.

North Carolina SB 1048

North Carolina adds numerous types of identifying information to the definition of "personal information," but only to the extent that such information would permit access to a person's financial accounts or resources. The North Carolina law defines a "security breach" as "an incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur, or that creates a material risk of harm to a consumer."

North Carolina mandates that reasonable measures be taken to protect its citizens' information and requires the measures to include means for appropriately disposing personal information. The state exempts entities subject to Gramm-Leach-Bliley and HIPAA from the disposal requirements.

North Carolina adds telephone notice as a means to notify individuals about a security breach and sets specific terms that must be included in each type of notice. In the event that more than 1,000 people are notified of a security breach pursuant to North Carolina law, the Consumer Protection Division of the Attorney General's Office must be notified, as well as all consumer reporting agencies. Financial institutions subject to the federal interagency guidelines developed under GLB are deemed compliant with this law. No private right of action may be brought by an individual for a violation of this law *unless* the individual is injured as a result of the violation.

North Dakota SB 2251

North Dakota tracks the California law but deems compliant those financial institutions and other entities subject to the federal interagency guidelines.

Rhode Island HB 6191

Rhode Island's law requires three distinct requirements to be in place in the event of any security breach. First, a business that deals with personal information (defined separately for these purposes as "any information that identifies, relates to, describes or is capable of being associated with a particular individual") must implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

Second, a business must contractually require third parties to maintain such security procedures if it is disclosing personal information about Rhode Island residents to them. Entities governed by HIPAA and those subject to greater federal protections are exempt from these pre-breach measures.

Third, Rhode Island requires businesses to maintain adequate destruction methods for personal information that make it unreadable. The state also has a distinct and detailed "shine the light" law that mirrors that of California by dealing with businesses that disclose personal information for use in direct marketing. Rhode Island, like California, provides a private right of action for violation of its security-breach law.

Tennessee HB 2170

Tennessee mandates notification of a security breach only if the personal information was "materially" compromised. Tennessee also requires notice to consumer reporting agencies when more than 1,000 people are notified of a breach. Tennessee exempts entities governed by Gramm-Leach-Bliley and provides a private right of action to individuals harmed by a violation of this law.

Texas SB 122

The definition of "sensitive personal information" in Texas follows the California definition of "personal information." Texas also adds two pre-breach measures: reasonable security procedures and appropriate document destruction methods for such information. Texas provides for notification to consumer reporting agencies in the event that more than 10,000 individuals are notified of a breach.

Washington SB 6043

The Washington law provides a threshold before notification is required. "A person or business under this section shall not be required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of criminal activity." A private right of action is established for individuals injured by a violation of this statute.

Compliance

Obviously, the best way to avoid disclosure under these laws is to avoid the breach in the first place. Therefore, for those seeking to comply with the new state security-breach laws (as well as those sure to come), the first step is to ensure that an adequate privacy and information security policy is adopted and that procedures are put in place to make it effective. Such a comprehensive program, if intended to meet the highest common denominator of the new laws, should include reasonable security measures, contractual obligations on third parties that require reasonable security measures, data destruction procedures appropriate for personal information and the utilization of encryption to ensure the safe transfer of personal information to third parties. Additionally, a security-breach response procedure that provides a plan for expediently notifying individuals of any breach should be implemented.

State-by-state compliance may not be practical. An entity dealing with a breach would need to examine whether the breach is the type governed by each state's law, whether the information at issue falls within the definition of "personal information" in each state where it does business and whether it would be subject to any of the exemptions. In the states that require notification of a breach only if there is a reasonable risk of harm, an entity will have to examine closely the standards for determining the risk in each state.

What are the true definitions of the phrases "reasonable likelihood of harm," "not likely to result in harm," "materially compromised" and a "technical breach"? This question is being hotly debated on the federal level right now as Congress reviews various federal bills calling for a national security-breach standard. Most states that have incorporated a "threshold" showing of harm will also require an investigation. What constitutes a "reasonable investigation"? States such as Connecticut require consultation with federal, state and local agencies when determining if there is a reasonable risk of harm in the event of a security breach.

Likewise, state-by-state compliance would require a close look at the specific pre-breach measures dictated by each state, such as data destruction requirements, contractual protections for transfer, reasonable security measures and encryption for any data relating to citizens of those states. This task alone would prove difficult for companies doing business throughout the United States.

As this list of considerations demonstrates, adopting a "minimum compliance" approach tailored to each state could be much more burdensome than striving for uniform compliance with the highest applicable standard. Given the prevalence of comprehensive privacy laws elsewhere in the world and the growing number of privacy protections in the United States, a privacy policy that adopts the highest standards may often be the better route.

Any compliance program would start with an assessment of current privacy practices by asking questions such as:

- What personal information is collected?
- Why is it collected?
- How is it collected?
- How is it used?
- Are data subjects apprised of the uses?

- Is comment sought?
- Where is it stored?
- Who has access?
- What security measures are used to protect it?
- To whom is it disclosed or transferred? and
- When and how is it disposed of?

Once a business has assessed its data-gathering priorities and existing privacy protections, it can then determine the steps necessary to advance a program to achieve broad compliance. Developing a privacy program requires a broad understanding of how an organization works and its overall culture, as well as some general technical savvy.

Generally, a privacy program should include physical, technological and administrative safeguards to protect personal information:

- Allow employees access to only the limited categories of personal information their job responsibilities require;
- Use technological means to restrict internal access to personal information whenever possible;
- Monitor employee access to higher-risk personal information;
- Immediately remove the access privileges of former employees and contractors;
- Provide training to promote awareness of privacy policies and procedures;
- Require appropriate security and privacy procedures in contracts with third-party service providers and vendors that handle personal information on the company's behalf;
- Use intrusion-detection technology to ensure rapid detection of a breach;
- Use data encryption, whenever possible, particularly when personal information is transferred;
- Establish a system of disposal for records containing personal information that renders such information indecipherable, *e.g.*, cross-cut shredding and "wiping" hard drives;
- Establish a system of disposal for records containing personal information that provides for their disposal in a timely manner, *i.e.*, only as long as necessary; and
- Establish a response plan that includes specific notification procedures and timing in the event of a security breach.

Embedding procedures such as these into corporate practices and generally changing culture with respect to the treatment of personal information will go a long way toward ensuring compliance with privacy laws in the United States and across the globe.

The trend is toward greater privacy protection around the world. Even if U.S. laws do not legally impose the rigorous type of constraints found in Europe, public awareness of privacy issues is on the rise and individuals are just beginning to exercise their legal rights when their personal information is compromised.

Conclusion

The security-breach-notification laws now in place require more than just a cursory glance at where business is done and when notification is required. Many states have added pre-breach protections for personal information that must be put into place immediately. Additionally, the varying standards for when a breach must be reported make compliance difficult.

Even if a federal law is passed, there is no special formula for distinguishing a harmful breach from one that is not, which is why many prefer the California-style liability standard — if there is a breach, notification is required regardless of negligence or likelihood of harm. Establishing policies and procedures that protect personal information and help to prevent a breach will certainly lessen the likelihood that notification will be required.

** Robin Campbell is a member of Crowell & Moring's privacy and data protection team. She specializes in the development and implementation of global information management strategies for the handling of personal data, including employee, customer and consumer information. Prior to joining Crowell & Moring, Campbell worked in Geneva as a special consultant to Hewlett-Packard Europe during the early stages of the European Data Protection Directive's implementation. Gaela Bailey, an associate at Crowell & Moring's London office, contributed to this article.*