Privacy, Network Security, and the Law

By Julie Machal-Fulks and Robert J. Scott

SCOTT & SCOTT
COMPLIANCE SIMPLIFIED

SCOTT & SCOTT

COMPLIANCE SIMPLIFIED

Privacy, Network Security, and the Law

By Julie Machal-Fulks and Robert J. Scott

Introduction

In the four years since California took the lead and enacted SB 1386, many states have followed suit and enacted similar legislation. While many of the provisions are similar, the laws contain varying definitions of personal information. The laws also provide for different types of notification after a security breach. Although this article will include a brief discussion of various state statutes, the differences between the various state laws may be made irrelevant by federal legislation. There are five bills currently under consideration by Congress. It is unclear which, if any, of the pending bills will become the national security breach notification law. What is clear is that if any of the current iterations of the pending legislation is enacted by Congress, businesses will once again have to adapt their business practices because the federal legislation will preempt the current state laws.

I. Overview of State Legislation

a. Definition of Personal Information.

The primary element of the privacy breach notification statutes in the various states is the definition of personal information. Generally, any business that possesses the personal information of a resident of a particular state must notify the resident that his or her personal information has been obtained by an unauthorized individual. Obviously, to determine whether a breach must be reported, it is critical to determine whether information obtained by a hacker qualifies as personal information for purposes of the many different state statutes.

For instance, in California, personal information includes a person's first name or first initial and last name, along with one of the following unencrypted pieces of information:

- social security number;
- driver's license number or state identification number; or
- account number, credit card number, or debit card number, combined with any password, security code, or access code.[1]

The definitions of personal information in Connecticut, Delaware, Florida, Illinois, Louisiana, Minnesota, Montana, Nevada, New Jersey, Rhode Island, Tennessee, Texas, and Washington are identical to California's definition.[2] Although Indiana's and Ohio's definitions of personal information are identical to California's definition, the notification statutes in these states only apply to state agencies.[3] Private businesses are not required by the Indiana or Ohio statutes to report security breaches.

There are also several states that include more information in the definition of personal information than California. For example, Arkansas' statute contains medical information, as well as the items enumerated in the California definition of personal information.[4] Georgia's and Maine's definitions of personal information include the data components identified in California's statute, as well as account passwords or other personal identification numbers or access codes and any items that, even without the first and last name are sufficient to allow an unauthorized person to attempt identity theft.[5]

Businesses generally cannot reduce their reporting onus by requiring customers to waive their notification rights.

North Carolina's statute also expands the California definition to include passport numbers, debit card numbers, digital signatures, any other numbers or information that can be used to access a person's financial resources, biometric data, and fingerprints.[6] North Dakota also includes date of birth, mother's maiden name, identification numbers assigned by employers, and digital signatures.[7] In New York, "personal information" is defined as information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person. Notification is required when public information is obtained in conjunction with a social security number, driver's license or state identification number, or account number, credit card number, or debit card number, in combination with the security code or password.[8]

Businesses that maintain personal information on behalf of clients can significantly reduce the burden of reporting security breaches by encrypting the data. Of the twenty-three states that have enacted security breach notification laws, only five states require notification of a breach of encrypted data.[9]

Businesses that expect to incorporate provisions into their customer contracts waiving the statutory notification provisions should beware. Most privacy breach notification statutes include provisions that any attempt to waive the statutory obligations is void because it is against public policy. For more information regarding the other components of the state statutes, please refer to Figure 1.

b. Notification After Personal Information Has Been Breached.

Most of the jurisdictions also followed California's lead when describing the type of notice required for security breaches. The vast majority of states allow written notice or electronic notice provided in accordance with 15 U.S.C. § 7001. If the person or business providing the notice demonstrates that the number of affected persons exceeds 500,000 or that the cost of notice would exceed $250,000, then notice may be provided via electronic mail, via posting on the person or business' website, or via publication in major statewide media.

Five states allow telephone notification in addition to the notice described above. Delaware, Maine, Montana, North Carolina, and Pennsylvania allow notification via telephone, with varying degrees of restrictions. For instance, Maine requires those providing telephonic notice to maintain a log, Pennsylvania only allows telephonic notice if the customer can reasonably be expected to receive the notice and it is given in a clear, conspicuous manner, and North Carolina requires that contact be made directly with the affected person.

II. Pending Federal Legislation

a. The Notification of Risk to Personal Data Act.

The proposed Notification of Risk to Personal Data Act (NRPDA) was introduced in the Senate on June 28, 2005 by Senator Jefferson Sessions [R-AL].[10] The bill, which has been approved in committee and is not before the entire Senate, is the legislation currently pending in the Senate that is most like the California statute. The bill would preempt all the state notification laws and would require notification if there is a breach of sensitive personal information that results in a significant risk of identity theft to any individual. Notification must be made as expediently as possible and without unreasonable delay.

The definition of sensitive personal information differs slightly from that of the states. For purposes of the NRPDA, sensitive personal information includes an individual's first and last name, the individual's address or telephone number, and the social security number, driver's license or state identification number, financial account number, credit or debit card number and any required security or access code or password. Like many state laws, the NRPDA excludes publicly available information and encrypted information from the definition of sensitive personal information. Similarly, notification is not required if notification would impede a civil or criminal investigation.

Under this legislation, notice could be given in writing, by telephone, e-mail, or in certain circumstances, by posting on the Internet or notifying the media. Before sending notice to more than 1,000 individuals, those required to give notice must also notify consumer credit reporting agencies as to the number of individuals impacted and the type of notice that will be given to individuals.

The most significant differences between the state security breach laws and the NRPDA are the enforcement provisions. Violations of the NRPDA would be enforced by the "functional regulator." The functional regulator is the appropriate government entity based on the type of agency or business that violated the provisions of the NRPDA. For instance, if an insurance agency violated the NRPDA, the state insurance authority would enforce the provisions; if an air carrier failed to comply with the provisions, the Secretary of Transportation would be the functional regulator. State Attorneys General could also bring actions in federal court for violations of the NRPDA. The proposed legislation prohibits private causes of action.

b. The Identity Theft Protection Act.

The proposed Identity Theft Protection Act (ITPA) is currently pending in the Senate.[11] It was introduced on July 14, 2005 by Senator Gordon Smith [R-OR] and is currently scheduled for debate. The ITPA expressly preempts all state and local laws governing security breach notification. The current version of the bill provides that a covered entity has to notify the Federal Trade Commission (FTC), possibly all credit reporting agencies, and possibly consumers of breaches in security. Covered entity is defined as "a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity, and any charitable, educational, or nonprofit organization that acquires, maintains, or utilizes sensitive personal information."

The sensitive personal information definition in the ITPA is similar, but not identical to, California's definition. Sensitive personal information is an individual's name, address, or telephone number combined with one or more of the following pieces of information:

- social security or other taxpayer number;
- financial account number, credit card number, or debit card number, combined with the required security code, access code, or password; or
- state driver's license identification number or state resident identification number.

Unlike the state laws, covered entities would be required to notify various agencies based on the number of individuals affected by the breach. If 1,000 or more individuals are affected by the breach, the covered agency must report the breach to the FTC, as well as all of the consumer credit reporting agencies. If fewer than 1,000 individuals are impacted and if the covered entity determines that the breach does not create a reasonable risk of identity theft, the covered entity must report

Figure 1: State Statutes

State	Time to Notify Consumers of a Breach of Personal Information	Civil Penalties for Failure to Promptly Notify Customers of Breach	Private Right of Action*	Exemption for Encrypted Personal Information	Exemption for Criminal Investigations or Information Publicly Available from Government Entities	Exemption for Immaterial Breaches (Typically Defined as No Reasonable Likelihood of Harm)
Arkansas	Most expedient time possible, without unreasonable delay	●		●	●	●
California	Most expedient time possible, without unreasonable delay		●	●	●	
Connecticut	Immediately			●	●	●
Delaware	Immediately, in the most expedient time possible, without unreasonable delay	●	●	●	●	
Florida	Without unreasonable delay	●		●	●	
Georgia	Most expedient time possible, without unreasonable delay			●	●	
Illinois	Most expedient time possible, without unreasonable delay		●	●	●	
Indiana	Without unreasonable delay			●	●	
Louisiana	Most expedient time possible, without unreasonable delay		●		●	●
Maine	Most expedient time possible, without unreasonable delay	●		●	●	
Minnesota	Most expedient time possible, without unreasonable delay	●		●	●	
Montana	Without unreasonable delay	●		●	●	
Nevada	Most expedient time possible, without unreasonable delay	●	●	●	●	
New Jersey	Most expedient time possible, without unreasonable delay			●	●	●
New York	Most expedient time possible, without unreasonable delay	●				
North Carolina	Without unreasonable delay	●	●		●	●
North Dakota	Most expedient time possible, without unreasonable delay			●	●	
Ohio	Most expedient time possible, but not later than 45 days	●			●	●
Pennsylvania	Without unreasonable delay	●		●	●	
Rhode Island	Most expedient time possible, without unreasonable delay	●	●	●	●	●
Tennessee	Most expedient time possible, without unreasonable delay		●	●	●	
Texas	As quickly as possible	●			●	
Washington	Most expedient time possible, without unreasonable delay		●	●	●	●

**The private cause of action is assigned to the data collector whose information was breached against the party responsible for the breach.*

the breach to the FTC but not to the consumer reporting agencies.

Regardless of the number of persons affected, covered entities would also be required to notify consumers of the breach when there is a reasonable risk of identity theft. Notification pursuant to this provision must take place in the most expedient manner practicable, but not later than 45 days after the date the breach was discovered by the covered entity.

To determine whether there is a reasonable risk of identity theft, covered entities must consider a number of factors. The proposed legislation requires covered entities to evaluate whether the data contains sensitive personal information usable by an unauthorized third party and whether the data is in the possession and control of an unauthorized party likely to commit identity theft. The notice provisions related to consumers are very similar to the state provisions – written or electronic notice and substitute notice under certain circumstances.

Like the majority of state laws, under the ITPA, covered entities would not have to notify consumers of a breach when notice would materially impede a civil or criminal investigation or when notification would threaten national security. The ITPA would be enforced by the FTC, as well as other relevant federal agencies (e.g., the Securities and Exchange Commission would have power to enforce the ITPA with respect to broker/dealers). Although civil penalties are authorized under the ITPA, there would be no private right of action.

c. The Personal Data Privacy and Security Act.

The Personal Data Privacy and Security Act (PDPSA) is also currently pending in the Senate. It was introduced on September 29, 2005 by Senators Arlen Specter [R-PA], Russell Feingold [D-WI], Dianne Feinstein [D-CA], and Patrick Leahy [D-VT].[12] The bill has been sent by the committee to be considered by the entire Senate. The PDPSA does not apply to financial institutions, entities covered by HIPAA, or any business that qualifies for exemption under the Safe Harbor provision. The Safe Harbor provision exempts businesses that provide protection equal to industry standards, as identified by the FTC.

All other agencies or business entities engaged in interstate commerce that use access, transmit, store, dispose of, or collect sensitive personally identifiable information, would be required to notify any resident of the United States whose information has been, or is reasonably believed to have been accessed or acquired. This notification must be provided without unreasonable delay. Sensitive personally identifiable information is defined as an individual's first name or first initial and last name, and:

- a non-truncated social security number, driver's license number, passport number, or alien registration number;
- two of the following;
  - o home address or telephone number;
  - o mother's maiden name;
  - o complete birth day;
- fingerprint, voiceprint, retina or iris image, or any other unique physical representation; or
- a unique account identifier, electronic identification number, user name, or routing code, in combination with any associated security code, access code, or password.

Additionally, sensitive personally identifiable information includes a financial account number, credit card number, or debit card number, "in combination with any security code, access code, or password that is required for an individual to obtain money, goods, services, or any other thing of value."

The notification provisions would not apply to an agency, if the agency certifies in writing that notification may hinder an investigation or cause damage to national security. Businesses would not have to follow the notification provisions if a risk assessment indicates that there is no significant risk of harm to the individuals and the business notifies the Secret Service of the results of the risk assessment without unreasonable delay but not later than 45 days after the breach. Businesses would also be required to notify the Secret Service of their intent to invoke the risk-assessment exemption. The Secret Service would then have 10 days to compel the business to provide notice.

Businesses would not have to follow the notification provisions if a risk assessment indicated no significant risk of harm to the individuals

Businesses that are required to disclose security breaches under the PDPSA would be required to provide individual notice and media notice. The individual notice requirements would be satisfied by providing written notice, telephone notice to the individual personally, or e-mail notice if the individual consented to receive such notice. Additionally, if more than 1,000 individuals are involved, the agency or business must notify all consumer credit reporting agencies.

Additionally, the agency or business must give notice of the security breach to the Secret Service if the number of individuals affected exceeds 10,000, if the database accessed contains sensitive personally identifiable information of more than 1,000,000 individuals, if the breached database is owned by the federal government,

or if the sensitive personally identifiable information is that of federal government employees or contractors.

Like the ITPA, the PSPDA would completely preempt state laws regarding security breach notifications. The proposed legislation expressly prohibits private causes of action for injuries related to security breaches, but it does provide for civil penalties in actions instituted by the Attorney General.

d. The Financial Data Protection Act.

The proposed Financial Data Protection Act (FDPA) was introduced on October 6, 2005 by Representative Steven LaTourette [R-OH] and 14 co-sponsors.[13] This bill has not made it out of the House committee. Most bills do not progress from committee to the entire House. If passed, this legislation would also completely preempt all state security breach notification laws.

The FDPA would amend the Fair Credit Reporting Act. The FDPA requires consumer reporters to investigate potential breaches of sensitive personal information. Consumer reporter is defined as "any consumer reporting agency or financial institution, or any person which, for monetary fees, dues, on a cooperative nonprofit basis, or otherwise regularly engages in whole or in part in the practice of assembling or evaluating consumer reports, consumer credit information, or other information on consumers." Sensitive financial personal information includes a financial account number combined with an access, security, or biometric code or other password or personal identification information. It also includes the first and last name, address or telephone number, and any either a social security number, driver's license or identification number, or taxpayer identification number.

If the breach may result in substantial harm or inconvenience to any consumer to whom the information relates, the consumer reporter must promptly notify:

- the Secret Service;
- the appropriate regulatory agency;
- any entity that owns or is obligated on a financial account that may be subject to unauthorized transactions as a result of the breach;
- if the breach involves 1,000 or more consumers, each nationwide consumer reporting agency ; and
- any appropriate critical third party.

Consumer reporters must also provide notice to consumers if there is a breach that results in a reasonable probability that personal information may be misused. This notice must be made without unreasonable delay. If requested, the consumer reporter must make free credit monitoring services available to consumers for six months. Consumer reporters may delay notice if notice would impede a current civil or criminal investigation. The functional regulatory agencies would be responsible for enforcement of the FDPA.

e. The Data Accountability and Trust Act.

The proposed Data Accountability and Trust Act (DATA) was introduced on October 26, 2005 by Representative Clifford Stearns [R-FL] and 8 co-sponsors.[14] It also has not progressed from the committee and would preempt state law.

The DATA would require any person engaged in interstate commerce to (1) report a breach of security to every individual whose personal information was acquired by an unauthorized source, (2) to notify the FTC, (3) to place a conspicuous notice on the Internet website of the person, and (4) if the breach involves financial account information, to notify the financial institution that issued the account. Notification must be made as promptly as possible and without unreasonable delay. Persons could notify individuals of the breach in writing or via electronic mail, and the proposed law would also allow substitute notification if certain criteria were met.

For purposes of the DATA, personal information includes an individual's first and last name and any one of the following:

- social security number;
- driver's license number or other state identification number; or
- financial account number, credit card number, debit card number, and any required security code, access code, or password.

This proposed legislation would require each person providing notification to individuals to also provide a free copy of the individuals' credit report from at least one major credit reporting agency.

The FTC would enforce violations of the DATA. Although the bill would preempt state notification laws, it specifically excludes from preemption actions based on state trespass, contract, and tort laws as well as other state laws relating to acts of fraud. In other words, if this legislation were enacted, individuals might be able to seek redress under state law for injuries resulting from unauthorized disclosure of their personal information.

III. The New Standard of Care – How to Avoid Liability

Security breaches can be costly. In the past several months, the FTC has investigated and sanctioned several companies for lapses in security involving customer information. For instance, Superior Mortgage Company was accused of misrepresentation by the FTC because it claimed its data was encrypted, but the information was decrypted before it was transmitted via electronic mail to its headquarters.[15] Superior Mortgage agreed to

refrain from making misrepresentations and submitted to FTC monitoring for 10 years. DSW was sanctioned for storing unencrypted files that were easily accessed using a commonly known user name and password. DSW agreed to implement comprehensive security measures and submit to FTC compliance monitoring for 20 years.[16] ChoicePoint agreed to pay the $15 million in fines and restitution and allow 20 years of monitoring after it provided sensitive personal information to subscribers who did not have a permissible purpose.[17]

Based on the current state laws it is clear that businesses should, at the very least, ensure that all names, addresses, account numbers, and other personal information of consumers is encrypted. This will minimize the risk that the business will have to notify consumers or law enforcement agencies should a breach occur. Until federal legislation is enacted, businesses must also be aware of the various state law statutes governing the protection of data to determine whether they meet the standards. It may be useful to regularly consult with your attorneys regarding the requirements in the relevant jurisdictions. Ensuring that you comply with the statutes governing the storage of information will also decrease the risk of liability.

...it is clear that businesses should, at the very least, ensure that all names, addresses, account numbers, and other personal information of consumers is encrypted.

Although many state laws do not allow private causes of action based on the security breach laws, other claims based on breach of contract, misrepresentation, or negligence may not be precluded. For instance consumers in many states can file lawsuits against companies whose security was breached, claiming that the companies negligently stored or protected the information. In addition to being diligent about data protection, companies should also review their contracts and sales materials to ensure that in addition to meeting all the statutory requirements, they are also fulfilling all of their promises to their customers.

Conclusion

Until federal legislation creates a uniform standard and possibly prohibits private causes of action for security breaches or notifications thereof, businesses must constantly familiarize themselves with the ever-evolving notification requirements for each state in which they do business. With diligent efforts, companies can reduce the possibility of liability for breaches in security.

Notes

[1] Cal. Civil Code, § 1798.82(e).

[2] Connecticut General Statutes § § 36a-701b(a); 6 Delaware Code § 12B-101, Florida Statutes § 817.5681(d)(5); 815 Illinois Compiled Statutes § 530/5; Louisiana Revised Statutes § 51:3073(4); 10 Maine Revised Statutes § 1347(6); Minnesota Statutes § 325E.61(e); Montana Statutes § 30-14- 1704(4)(b); Nevada Revised Statutes §603A.040; New Jersey Statutes § 56:8-161; 73 Pennsylvania Statutes § 2302; Rhode Island General Laws § 11-49.2-5(c); Tennessee Code § 47-18-2107(a)(3); Texas Business & Commerce Code §§ 48.002, 48.103; Washington Revised Code § 19.255.010(5).

[3] Indiana Code § 4-1-11-3; Ohio Revised Code § 1349.19(A)(7).

[4] Ark. 4-110-103;

[5] Georgia Code § 10-1-911(5), 10 Maine Revised Statutes § 1347(6).

[6] North Carolina General Statutes §§ 75-61(10), 14-113.20(b).

[7] North Dakota Statutes § 51-30-01(2)(a).

[8] New York General Business Law § 899-aa(1)(a)-(b).

[9] Louisiana, New York, North Carolina, Ohio, and Texas have enacted statutes that require notification even if the personal information data is encrypted.

[10] Notification of Risk to Personal Data Act, S.B. 1326, 109th Cong. (2005).

[11] Identity Theft Protection Act, S.B. 1408, 109th Cong. (2005).

[12] Personal Data Privacy and Security Act, S.B. 1789, 109th Cong. (2005).

[13] Financial Data Protection Act, H.R. 3997, 109th Cong. (2005).

[14] Data Accountability and Trust Act, H.B. 4127, 190th Cong. (2005).

[15] *In the Matter of Superior Mortgage Corporation, FTC Docket No. C-4153 (December 14, 2005).*

[16] *In the Matter of DSW, Inc., FTC Docket No. C-4157 (March 7, 2006).*

[17] *United States v. ChoicePoint, 1:06-CV-0198 (N.D. Ga. 2006).*

SCOTT & SCOTT

COMPLIANCE SIMPLIFIED

2200 Ross Avenue :: Suite 5350 East :: Dallas, Texas 75201 :: t 800.596.6176 :: f 800.529.3292 :: scottandscottllp.com