ASPEN PUBLISHERS

The Computer & Internet Lawyer

Volume 26 ▲ Number 9 ▲ SEPTEMBER 2009

Ronald L. Johnston, Arnold & Porter, LLP Editor-in-Chief*

Data Security Requirements Evolve: From Reasonableness to Specifics

By Lothar Determann and Jesse D. Hwang

Government agencies and businesses around the world have been subject to data privacy and security legislation for decades.[1] Historically, most laws have focused on consent and notification requirements, as well as substantive limitations on the collection, use, and transfer of personal data. Relatively few statutes have expressly addressed requirements pertaining to entities' data security safeguards; and, those that have legislated on the issue have simply set forth a general reasonableness standard. But, when California enacted the world's first data security breach notification law in 2003[2] and companies started reporting security breaches *en masse*, the great threat that lax security standards pose to personal privacy and other individual interests became abundantly clear to the public. Since then, most US states have followed California's lead and passed data security breach notification laws. More recently, lawmakers in the United States and elsewhere have started prescribing very specific technical and organizational measures intended to ensure that companies take more comprehensive steps to prevent security breaches and protect the data and privacy of consumers, employees, and other individuals. Businesses of all sizes and industry sectors should take note of these evolving new rules in order to comply with applicable laws and mitigate the risks of devastating security breaches.

The extent to which businesses collect, store, manipulate, transfer, and otherwise process personal data depends on their business needs and legal obligations to collect and retain information. All businesses process *some* personal data; at a minimum, they handle contact information of their own employees, customers, and business partners. Most businesses also process more sensitive data, such as payroll information, consumer purchase histories, data from credit card transactions, and other financial and medical data.

Prof. Dr. Lothar Determann is a partner with Baker & McKenzie's San Francisco/Palo Alto office, where he focuses on international technology and business law; he also teaches technology and privacy law courses at UC California, Berkeley School of Law (Boalt Hall) and the Free University of Berlin, Germany. **Jesse D. Hwang** is an associate in the San Francisco office of Baker & McKenzie and focuses on data privacy and technology law.

Wolters Kluwer
Law & Business

Because no two companies share the exact same business focus, data processing practices, or threats to data security, each finds itself in a unique position to determine appropriate data security measures for itself. Because security threats are constantly evolving, it is no surprise that legislatures and enforcement agencies have initially addressed data security threats by requiring entities that process personal data to implement "reasonable" security safeguards at first, and then developing more specific requirements for certain industries, data categories, and transaction types. These first-generation data security laws helped identify issues and generate a general public awareness, but triggered little proactive planning from most businesses. Most companies either found themselves outside of the law's scope or tended to consider their measures reasonable until a security breach occurred. Consequently, outside highly regulated industry sectors, data security measures have historically been largely *ad hoc* and incident-driven as opposed to holistic and strategic. More recently, however, data security laws have become increasingly detailed as to required measures and broad as to covered entities. A new generation of data security laws requires relatively specific security measures from virtually all businesses.

In this article, we will provide an overview and update on data security laws with a particular focus on the new generation of legal requirements that have been recently enacted in state legislatures and some foreign countries.

Federal Law

Federal law is currently sectoral in nature in that the extent to which data security safeguards are regulated depends on the types of personal data, data subjects, and industry sectors at issue. Currently, the federal data security regime encompasses both statutes that prescribe specific security safeguards and those based on a general reasonableness standard. The Health Insurance Portability and Accountability Act (HIPAA), for example, applies primarily to health care companies and prescribes specific administrative, physical, and technical safeguards along with required and suggested implementation specifications to meet HIPAA standards.[3] The Gramm-Leach-Bliley Financial Services Modernization Act, in addition, contains a Safeguards Rule that sets forth fairly specific security requirements for businesses that provide certain financial services or products.[4] Federal laws that require data security safeguards under a relatively flexible reasonableness standard include the Children's Online Privacy Protection Act, which aims to protect information collected from children online.[5]

Beyond such sectoral requirements, the Federal Trade Commission (FTC) has pursued data security risks and breaches as incidents involving "unfair or deceptive"[6] practices.[7] Historically, the FTC has brought such actions under a deception theory of liability, arguing that breaches of representations by businesses to consumers to protect personal data constitute deceptive trade practices.[8] More recently, the FTC has pursued businesses under an unfairness theory of liability, arguing that simply failing to reasonably protect personal data constitutes an "unfair" business practice.[9] While enforcement generally concerns consumer-related data, the FTC has the power to take action against businesses that experience security breaches involving personal data of any kind, including employee data, for example.[10] FTC consent orders typically enjoin businesses from making deceptive representations in the future and require the implementation and maintenance of a data security program and independent security audits for a number of years.[11]

Security measures do not have to be foolproof to be FTC compliant; rather, they must reasonably protect personal data.[12] While 15 U.S.C. § 45 does not define "unfair," "deceptive," or "reasonable," the following practices are generally considered a violation of that provision and an unreasonable risk of a security breach, based on FTC enforcement actions to date:

- Weak passwords to computer systems;
- Employees who are untrained in data security or privacy;
- Unnecessary retention of personal data;
- Insufficient data discarding practices;
- Unsecured mobile devices;
- Sporadic security audits and investigations;
- Inadequate methods to detect unauthorized access to data; and
- Storage of sensitive data in readable, accessible, or unencrypted form.[13]

General Tort Liability

Businesses that fail to protect data can be liable under common law tort principles. These principles, by their very nature, do not specify the security measures required to maintain a successful action and instead operate according to general concepts, such as duties of

care, reasonableness, and negligence. Individuals may sue under a tort theory of negligence if they can prove that

1. The defendant had a duty to secure the personal data or system;

2. The defendant breached that duty;

3. The breach was the proximate cause of harm to the plaintiff; and

4. The plaintiff suffered actual harm or damages.[14]

In January 2007, for example, a class action was filed against TJX after a security breach involving thousands of customers, who alleged that TJX did not disclose the breach for more than a month and was negligent in protecting the personal data.[15] But, courts have been hesitant to find standing and damages except when plaintiffs can show actual harm. Determining the amount and type of injury that is necessary for a *prima facie* case will be a key issue in future negligence-based cases.[16]

Whether and to what extent businesses have a duty, from a tort law perspective, to implement security measures to protect personal data is not yet settled. But, given the growing number of industry standards and data security laws (as discussed in this article), it seems likely that lawsuits will eventually establish that such duties of care exist, especially when statutory requirements like the HIPAA Security Rule directly apply.[17]

Industry Regulation

Some industry groups require very specific data security standards and sanction participating businesses that do not comply. The Payment Card Industry Data Security Standard (PCI DSS), for example, is comprised of administrative, physical, and technical safeguards and is used around the world to protect organizations that process credit card holder data from security vulnerabilities such as fraud and hacking. Any company processing, storing, or transmitting credit card holder data pertaining to any card branded with the logos of JCB International, Discover Financial Services, American Express, Visa, Inc., or MasterCard Worldwide must be PCI DSS-compliant. Non-compliant companies risk losing their ability to process credit card payments and being fined and audited.[18]

Foreign Laws

Entities in the United States can also be subject to foreign data security standards if they receive and process personal data from jurisdictions abroad, especially member states of the European Economic Area (EEA). In general, transfers of personal data from the EEA to the United States are prohibited by Directive 95/46/EC, even in the intercompany context. The Directive is very broad in scope and applies to all industry sectors, types of businesses, and categories of personal data.[19] Data transfers are generally prohibited, unless certain conditions are met, including the following:[20]

- The data controller[21] in the EEA and the recipient in the United States adhere to a data transfer agreement that incorporates model clauses[22] approved of by the EC Commission.

- The recipient in the United States adheres to the US/EU safe harbor[23] privacy principles and has completed a self-certification with the US Department of Commerce regarding the same.

Most states generally regulate data security with statutory provisions that require safe data handling practices and/or notification in case of a security breach.

In both cases, the recipient in the United States has obligations to protect the personal data received from the EEA. One of the safe harbor principles pertains to data security and requires participating organizations to implement "reasonable precautions."[24] Similarly, in both the controller-to-processor[25] and controller-to-controller versions of the model clauses, recipients must implement technical and organizational safeguards that are "appropriate" for the risks associated with the contemplated processing and the nature of the personal data to be protected.[26] There is no definition of "reasonable precautions" or "appropriate" in either the safe harbor privacy principles or the model clauses, respectively. Accordingly, there is little explicit guidance in these materials on the administrative, technical, or physical safeguards that would be required or would meet European standards. With respect to safe harbor, guidance from the FTC would probably be the most persuasive, since currently only entities that are subject to the authority of the FTC or US Department of Transportation may participate.

In the case of the model clauses, the term "appropriate" would probably be interpreted under the law of the EEA jurisdiction in which the data exporter is established, as stipulated by the model clauses on the issue of governing law.[27] Section 9 of the German Federal Data Protection Act, for example, requires "technical and organizational measures" to secure compliance

with substantive statutory requirements and refers to an attachment within the statute that lists certain protection concepts, albeit no specific technical measures.[28] The 2007 revisions to the Spanish Data Protection Act go into more detail and define various documentation, authentication, access control, and other security measures.[29] Italian law goes into yet more details and regulates, for example, how often companies must reset the passwords of users who have electronic access to sensitive versus non-sensitive data.[30]

Data Security Requirements of US State Laws

In the United States, most states generally regulate data security with statutory provisions that require safe data handling practices and/or notification in case of a security breach. Like those at the federal level, state data security laws are either generally applicable and vague (*i.e.*, the "reasonableness" standard) or sectoral and specific, varying by type of personal data, data subject, and industry.

Data Security Breach Notification Laws

Typical state security breach notification laws generally require businesses in their respective jurisdictions to notify affected residents if unencrypted personal data under the businesses' control is acquired in an unauthorized manner. The first such law was enacted in California in 2003,[31] and it has influenced the passing of similar legislation in 43 other states. Earlier this year, new laws were enacted in South Carolina[32] and Alaska,[33] bringing the total number of states that do not have any kind of security breach notification law to six: Alabama, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota.[34]

States with such laws typically differ in the scope of personal data that is covered, the requirements on the notification's timing, whether notice to authorities or other consumer-reporting agencies is required, penalties and enforcement, requirements on the notifications' content, and the exact situations in which notification is necessary. In general, the states provide an exemption from notification requirements if the personal data that was compromised was encrypted (so long as the encryption key was not compromised as well).

Although these laws do not discuss any particular data security safeguards, these notification laws motivate businesses to improve (or at least implement *some*) security measures in order to avoid the costs and bad publicity that can be associated with data breach and non-compliance. These laws also aim to prevent instances of identity theft and other forms of fraud by putting victims and the authorities on notice shortly after a breach occurs.

Recent developments indicate a possible trend toward more demanding state security breach laws. In Texas, the governor signed a bill on June 19, 2009, effective September 1, 2009, that adds health/medical information and information on the payment of health care to the scope of data covered by the state's security breach notification law.[35] Few other states have similar provisions for this type of personal data.[36]

Maine's governor also signed legislation recently, on May 19, 2009, limiting to seven days the time that a breach notification may be delayed following a determination by law enforcement that notification will not compromise a criminal investigation. Prior legislation merely stated that notification could be delayed in light of pending criminal investigations, but did not specify a timeframe for notification.[37]

Recent developments indicate a possible trend toward more demanding state security breach laws.

Perhaps more significantly, California's legislature is currently considering updating its pioneering security breach notification law by setting forth requirements for the contents of notifications, which many state laws do not do.[38] In particular, the proposed language would amend the prior law by requiring that any entity that must issue notice include in the notification:

- The name and contact information of the entity;
- A list of the personal information at issue;
- The date or estimated date of the breach,
- The date of the notice;
- Whether notification was delayed as a result of a criminal investigation;
- A general description of the breach;
- The estimated number of persons affected by the breach; and
- Contact information for the major credit reporting agencies if the breach involved a bank account or credit card number, a Social Security number, or a driver's license or California ID card number.

The proposed language also gives business entities the option to disclose:

- Information about what the entity has done to protect the victims; and
- Advice on how a victim can further protect himself or herself.

New York is also considering a bill that expands the content of security breach notifications to include:

- Contact information for the entity that experienced the breach;
- Information concerning steps taken to mitigate risks of identity theft;
- Contact information for the Consumer Protection Board; and
- Information on steps that individuals can take to protect against identity theft.

Furthermore, both California's and New York's proposed laws contain provisions that expand involvement of government authorities in cases of security breaches. California's proposals, for example, would amend prior law by requiring entities that must provide notification to more than 500 California residents as a result of a single breach to also submit notice to the state Attorney General. Similarly, according to New York's bill, entities that experience breaches of computerized data affecting more than 500,000 people would be required to provide a second notification within 120 days of the initial notice to the Cyber Security and Critical Infrastructure Coordination, Consumer Protection Board, and the Office of the Attorney General in order to allow those agencies to evaluate the response.[39]

Legislation in Minnesota,[40] though not a notification law, imposes statutory liability on retailers in case of a security breach. Specifically, this legislation (the first of its kind) makes it illegal for merchants to retain certain kinds of card data, such as cardholders' personal identification numbers (PINs), for more than 48 hours after a transaction is authorized. If an entity is non-compliant and there is a breach of that entity's (or that entity's service provider's) system, then that entity is required to reimburse financial institutions for "reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders." Although the statute provides a list of such costs, for example, refunds for illegal charges, costs of replacing cards, and costs of notifying consumers, it is not exhaustive, implying that merchant liability under the new law may be extremely broad. In particular, non-compliant entities are liable for costs from damages paid by financial institutions to cardholders injured by a breach. (The statute became effective on August 1, 2007, with respect to data retention and on August 1, 2008, regarding liability for security breaches).[41] Other US states have not followed Minnesota's lead in this respect, perhaps because they perceive financial institutions less as victims and more as the cause of problems, given relatively lax lending and credit card issuance practices by some institutions.[42]

Existing State Laws Requiring Data Security Safeguards

Rather than mandating specific administrative, physical, or technical security safeguards, state statutes that regulate data security have primarily done so with a reasonableness standard.[43] In California, for example, a "business that owns or licenses personal information about a California resident shall implement and maintain *reasonable* security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[44] Similarly, Nevada currently requires all business entities that "maintain records which contain personal information of a resident of [Nevada]" to "implement and maintain *reasonable* security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."[45]

As to the question of what is "reasonable" within the meaning of the state statutes, state agencies offer some opinions, guidance, and recommendations. California's Office of Information Security and Privacy Protection (OISPP) not only assists individuals with privacy-related concerns and coordinates with law enforcement but also recommends information-handling practices to businesses and policy changes to the state government.[46] Web sites for both the OISPP and Nevada's Bureau of Consumer Protection link to the Federal Trade Commission's (FTC) Web site for guidance on safeguarding personal data.[47]

Beyond such general requirements, businesses in both states that disclose personal information (as they define that term) about residents to third parties must do so pursuant to a contract in which the third party agrees to also implement and maintain reasonable security practices.[48] In California, businesses are required to take reasonable steps to destroy customer records with personal information that no longer needs to be retained,[49] and businesses may not require individuals to transmit their Social Security numbers over the

Internet unless the connection is secure or the data is encrypted.[50]

Current Nevada law, in particular, sets forth a specific duty to implement technical safeguards: A business must encrypt certain consumer data if it electronically transmits the data outside of the business's secure network (by means other than facsimile).[51] Currently, Nevada law does not require businesses to encrypt the same information if it is merely stored, for example, on a laptop, so long as it is not transmitted. Encryption also provides a safe harbor under Nevada's security breach notification law, thus providing further incentive to encrypt personal information.[52]

Rather than mandating specific administrative, physical, or technical security safeguards, state statutes that regulate data security have primarily done so with a reasonableness standard.

Legislation from Oregon, on the other hand, represents a bridge between the first-generation laws that are based on a vague reasonableness standard and those of the next generation, which specify specific data security safeguards.[53] Section 646A.622 of the Oregon Revised Statutes, like the California and Nevada provisions, requires businesses that process consumer personal data to implement and maintain "reasonable" data security safeguards. This Oregon provision, however, sets forth a number of options that businesses may take to meet this standard, essentially codifying a definition of "reasonable." In particular, businesses subject to Oregon's law are deemed in compliance if they comply with the Gramm-Leach-Bliley Act,[54] HIPAA,[55] or a state or federal law that provides greater protection than the Oregon law.[56] Businesses are also considered compliant if they implement an information security program that includes certain administrative, physical, and technical safeguards enumerated by the statute.[57] These enumerated safeguards, however, are not as comprehensive as those prescribed by the Massachusetts Regulations discussed next.

New Massachusetts Regulations

Massachusetts' Office of Consumer Affairs and Business Regulation (OCABR) promulgated the Massachusetts Regulations[58] pursuant to the Chapter 93H[59] of the General Laws of Massachusetts in September 2008[60] and amended them in February 2009.[61] The Massachusetts Regulations are especially significant to the field of data security law as they forge a drastic departure from previous first-generation state legislation to requirements for *specific* administrative, physical, and technical safeguards on a comprehensive level.

Covered Entities

The scope of covered entities is broad, as the Massachusetts Regulations apply "to all persons that own, license, store or maintain personal information about a resident of [Massachusetts]."[62] The term "person" includes natural persons, corporations, and other legal entities.[63] Thus, the Massachusetts Regulations can cover even business entities outside of Massachusetts if they possess "personal information" about Massachusetts residents. As applied, then, the Massachusetts Regulations probably cover any business with employees or customers who reside in Massachusetts and any service provider or retailer, for example, that maintains relationships with such businesses. Compliance by covered entities is required on or before January 1, 2010.[64]

Covered Data

The scope of the data covered is limited to the term "personal information," meaning a Massachusetts resident's "first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: Social Security Number; driver's license number or state-issued identification card number; or financial account number, or credit or debit card number . . . ."[65] "Personal information," however, does "not include information that is lawfully obtained from publicly available information" or from government records lawfully made available to the public.[66]

In particular, the Massachusetts Regulations' requirement to implement and maintain an information security program applies to "any records" containing "personal information."[67] "Records" are defined broadly as "any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics," implying a broad scope of media to which the Massachusetts Regulations apply (including paper, electronic, or other forms of media).[68]

Summary of Obligations

The Massachusetts Regulations first and foremost require a covered entity to develop, implement, maintain, and monitor a "comprehensive, written information security program" in order to protect personal information records. The Massachusetts

Regulations seem to provide some degree of flexibility in whether a program is compliant by allowing covered entities to tailor them according to the size, scope, and type of covered entity, the entity's available resources, the amount of data to be implicated, and the need for security and confidentiality of the personal information at issue.[69] Nevertheless, the Massachusetts Regulations still enumerate a number of specific administrative, physical, and technical safeguards that must be implemented for all covered entities. A summary of the Massachusetts Regulations' requirements follows.[70]

Administrative Safeguards

- Educating and training employees on data security;
- Identifying and assessing risks to data security and confidentiality;
- Evaluating and improving current safeguards (including employee training, monitoring employee compliance, and detection/prevention tools for security system failures);
- Verifying that third-party service providers with access to personal information can and will apply compliant security measures;
- Identifying what records, computer systems, and media store personal information;
- Regular monitoring of the security program's operation;
- Annual review of security measures or whenever there is a material change in business practices;
- Documenting actions regarding breaches;
- Reviewing events and actions taken after incidents, if any, to make changes in business practices relating to data security;
- Appointing at least one employee to maintain the security program;
- Implementing policies that address storage, access, and transport of records off the business premises by employees;
- Imposing disciplinary measures for violation of the security program;
- Limiting the personal information collected and retention period to that reasonably necessary to accomplish the purpose of collection;
- Limiting access rights to those who need-to-know to accomplish the purpose of collection or comply with retention requirements under law.

Physical Safeguards

- Preventing terminated employees from accessing records;
- Implementing restrictions for physical access to records;
- Storing records in locked facilities, storage areas, or containers.

Technical Safeguards

Covered entities that *electronically* store or transmit personal information must also include the following in their written, comprehensive information security programs with respect to computer and wireless systems:[71]

- Secure user authentication protocols, including
  - — Control of user IDs and other identifiers;
  - — Secure methods for assigning passwords or use of identifier technologies, such as biometrics;
  - — Control of passwords so that their location or formats do not compromise data security;
  - — Restricting access to active users or user accounts;
  - — Blocking access to user identification after multiple unsuccessful attempts to gain access
- Secure access control measures that restrict access to records to those who legitimately need to know and assign unique IDs and passwords;
- Encryption of all transmitted records and files that will travel across public networks or transmit wirelessly to the extent technically feasible;
- Encryption of all personal information stored on laptops and other portable devices;[72]
- Monitoring of systems for unauthorized use of, or access to, personal information;

- Up-to-date firewall protection and operating system security patches;

- Up-to-date versions of system security agent software, patches, and virus definitions, including malware protection (or software that can be supported with the same).

Given the scope of the Massachusetts Regulations, achieving compliance will likely require significant resources. Covered entities will need time and organizational coordination to review and revise existing policies, as well as the means to implement the required technical measures. In particular:

- Businesses may have to engage external service providers to determine whether their encryption technology and other IT resources comply with encryption requirements (assuming there is no existing in-house IT staff or consultant).[73]

- Businesses may have to purchase new computer hardware or software depending on whether current equipment can run software that secures electronic records and can receive security updates.[74]

- Businesses may need to hire consultants to implement some of the required technical safeguards, such as user identification protocols, secure access control measures, and firewalls. If there are no in-house IT resources, then businesses will probably need to hire someone to provide these services/resources.[75]

Compliance efforts should be fairly demanding, especially since the Massachusetts Regulations address not only IT policy but also administrative safeguards that touch upon how covered entities deal with third parties and administer human resources. For example, the Massachusetts Regulations require reasonable steps to verify and ensure that service providers that have access to personal information can and will comply with the Massachusetts Regulations themselves. Thus, covered entities will have to perform more due diligence when engaging service providers and possibly renegotiate service contract terms. Indeed, a prior version of the Massachusetts Regulations required covered entities to contractually obligate service providers to maintain the safeguards and to obtain written certification of a compliant written, comprehensive information security in place prior to granting access to personal information.

Compliance could be disproportionately time-consuming and costly for smaller businesses. Massachusetts has recognized the demanding nature of its regulations. Because of current economic circumstances, in November 2008, OCABR initially extended the original compliance deadline of January 1, 2009, to assist businesses experiencing financial difficulties.[76] OCABR again extended the compliance deadline in February 2009 to the current January 1, 2010, date.[77]

The ultimate influence of the Massachusetts Regulations, however, is unclear at this point due to their relatively recent passage, but also because of a bill that was proposed in the Massachusetts legislature out of concerns regarding the regulations' enforceability and impact on small businesses. That bill[78] would amend Chapter 93H[79] of the General Laws of Massachusetts and prohibit OCABR from promulgating regulations that require entities "to use a specific technology or technologies, or a specific method or methods for protecting personal information." If the bill passes, the Massachusetts Regulations may be further amended to be less comprehensive or specific, and some particular provisions, such as those on data encryption, may be omitted altogether. Indeed, the Massachusetts Regulations' influence on other states will likely also be weaker if the bill passes because it also states that any "person who is required to comply with federal laws, rules, regulations, guidance, or guidelines safeguarding personal information is deemed in compliance" with Massachusetts data security law, effectively deferring to federal data security law that may or may not be as specific or comprehensive.

New Nevada Law on Data Encryption

As discussed already, current Nevada law requires "data collectors," defined broadly, to implement and maintain "reasonable" security measures to protect records of certain personal information.[80] While Nevada has not changed its general reasonableness standard, it has supplemented these requirements on May 30, 2009,[81] effective January 1, 2010,[82] with a new provision on data encryption requirements:

- Covered data collectors that process credit or debit card payments for goods or services must comply with the PCI DSS; and

- All other covered data collectors may not (1) move "data storage devices"[83] containing non-encrypted personal information outside the control of the data collector or its data storage service provider or (2) electronically transfer non-encrypted personal information (other than by facsimile) to a person outside the data collector's secure system.

In addition, previously Nevada prohibited only businesses in Nevada from electronically transferring

non-encrypted personal information of *customers* (other than by facsimile) to a person outside the secure system of the business in § 597.970.[84] The new provision repeals § 597.970 and expands the scope of Nevada's encryption requirement to *non-customer* personal information as well.

All businesses have to design and implement security programs that meet the ever-increasing minimum legal standards and sufficiently guard against business risks.

The provisions are significant developments in state law because they mandate encryption of personal information in transmission *and* in storage. No other state laws currently require encryption to this extent, besides the Massachusetts Regulations. Perhaps more importantly, the Nevada amendments define "encryption" by specifying encryption technology, and safeguards that protect the cryptographic keys, that are adopted by an established standards-setting body, such as the Federal Information Processing Standards issued by the National Institute of Standard and Technology (NIST).

Toward State Requirements on Specific Data Security Safeguards?

Some of the developments that we have discussed regarding new state data security laws seem to indicate trends toward more specific regulation of security safeguards for personal data categories that virtually all businesses must process.

First, the Massachusetts Regulations (depending on the outcome of pending legislation) will likely be an important nationwide standard by which businesses will be evaluated in the area of data security. On their face, they "apply to all persons that own, license, store or maintain personal information about a resident" of Massachusetts.[85] Because most businesses involved in interstate commerce process personal data about individuals from all over the country, the Massachusetts Regulations may have extra-jurisdictional effect on businesses located outside of Massachusetts. Due to the relatively unprecedented nature in which the Massachusetts Regulations comprehensively mandate specific data security safeguards, other state courts and legislatures may look to the Massachusetts Regulations for guidance when interpreting or making law. Because the Massachusetts Regulations may signal a nationwide trend toward comprehensive state regulation of businesses' internal data security safeguards, businesses everywhere should examine the Massachusetts Regulations and address their requirements. Whether the federal government will introduce harmonizing data security legislation remains to be seen. Legislators in both the House and the Senate are currently working on draft legislation that addresses data security.[86]

Second, because Nevada defines "encryption" to be PCI DSS-compliant or technology adopted by established standards setting bodies such as the NIST, [87] such guidance could be persuasive in other jurisdictions that require encryption or provide an encryption safe harbor for security breach notification laws but do not define that term precisely. Both the Massachusetts Regulations and the amended Nevada law, for example, require encryption of personal information in transit *and* in storage.[88] It is unclear, for example, what sort of commercial tools would satisfy the Massachusetts Regulations' encryption requirements, since their definition of the term makes no reference to technical specifications or an industry standard.[89]

Practical Implications for US Businesses

All businesses have to design and implement security programs that meet the ever-increasing minimum legal standards and sufficiently guard against business risks. Fewer and fewer companies can afford to ignore data security challenges based on exemptions from sectoral laws or confidence in their own reasonableness until an incident occurs. Given the arrival of more specific data security requirements, companies will have to move away from incident-driven *ad hoc* responses to strategic data security programs, document, verify, and audit their processes, acquire and maintain adequate technology for information security, investigate and negotiate the data handling practices of service providers, and implement other measures that meet legal requirements. As companies revise their security policies and address compliance monitoring and auditing, however, they should also take note to avoid violating the privacy rights of employees and others, a consideration that conflicts somewhat with data security.[90]

While some companies will find that the costs of compliance exceed their available resources and budgetary constraints, this should not prevent any organization from at least taking initial steps to assess risks and compliance shortfalls and address high-priority risks one at a time. Large domestic and international businesses, in particular, may opt to comply with the strictest requirements out of all the jurisdictions in which they operate so that they can uniformly use data across geographic regions and business lines despite diverging legal requirements across the United States and around the world. Such a strategy will protect the

entire organization more effectively, avoid a need to keep data and databases separate, and harmonize different practices throughout the organization.

Notes

1. The German State of Hessen passed the world's first data protection law in 1970, available at *http://www.hessen.de/irj/hessen_Internet?cid=098693b3bbacadc19b81045a1c2300f2* (last visited May 25, 2009), and was quickly followed by other German states and European countries. California also enacted privacy legislation in the early '70s. *See, e.g.*, the Song-Beverly Credit Card Act of 1971 (Cal. Civ. Code §§ 1747-1748.7); *see* Lothar Determann and Daniel Robyn, "Card Tricks," *The Daily Journal,* April 28, 2009.
2. *See* Cal. Civ. Code § 1798.82; *see also* Cal. Civ. Code § 1798.29.
3. *See* the security regulations pertaining to the Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. Part 164.
4. 15 U.S.C. §§ 6801-6809.
5. *See* the regulations pertaining to the Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2, 312.3(e), and 312.8 (requiring operators of certain websites and online services who collect or maintain personal information from or about their users or visitors to "establish and maintain *reasonable* procedures to protect the confidentiality, security, and integrity of personal information collected from children") (emphasis added).
6. "[U]nfair or deceptive acts or practices in or affecting commerce … are hereby declared unlawful." 15 U.S.C. § 45(a)(1). *But see* 15 U.S.C. § 45(a)(2) (excluding certain industries and entities from the Federal Trade Commission's enforcement powers under 15 U.S.C. § 45(a)(1)).
7. Data Security Handbook 127 (American Bar Association, Section of Antitrust Law 2008).
8. *Id*. at 127-128.
9. *Id*. at 129-130 (citing BJ's Wholesale Club, FTC Dkt. No. C-4148 (Sept. 2005), *http://www.ftc.gov/os/caselist/0423160/0423160.shtm*).
10. *Id*. at 132.
11. *Id*. at 128-129 (citing Guess?, Inc., FTC Dkt. No. C-4091 (Aug. 2003), *http://www.ftc.gov/os/caselist/0223260.shtm*; MTS d/b/a Tower Records, FTC Dkt. No. C-4110 (Aug. 2003), *http://www.ftc.gov/os/caselist/0323209/0323209.shtm*; Petco Animal Supplies, FTC Dkt. No. C-4113 (Apr. 2007), *http://www.ftc.gov/os/caselist/0323221/0323221.shtm*; Guidance Software, Inc., FTC Dkt. No. C-4187 (Apr. 2007), *http://www.ftc.gov/os/caselist/0623057/index.shtm*; Life is good, Inc., FTC File No. 072-3046 (Jan. 2008), *http://www.ftc.gov/os/caselist/0723046.shtm*).
12. *Id*. at 132.
13. *Id*. at 132.
14. *Id*. at 122-123.
15. *See* TJX, 41 Attorneys General Agree to Close States' Data Breach Investigations, 14 *Electronic Commerce & Law Report*, 936 (2009); Jenn Abelson, "TJX Faces Class Action Lawsuit in Data Breach," *Boston Globe* (Jan. 30, 2007), available at *http://www.boston.com/business/globe/articles/2007/01/30/tjx_faces_class_action_lawsuit_in_data_breach/*. The lawsuit was later settled. *See* the settlement Web site, available at *http://www.tjxsettlement.com/*.
16. A class action lawsuit against data broker Axicom was dismissed after the court ruled that there was no evidence of actual damages. The plaintiffs had alleged that consumer personal data collected after a security breach was used to send spam and junk postal mail. Data Security Handbook 122-123 (American Bar Association, Section of Antitrust Law 2008) (citing Bell v. Axicom Corp., Civil No. 4:06-CV-00485-WRW, 2006 WL 2850042 (E.D. Ark. 2006); *see also* Declan McCullagh & Anne Broache, "Class Action Suit Over ID Theft Tossed Out," *CNET News* (Oct. 12, 2006), *http://news.com.com/2100-7348_3-6125028.html*). A similar class action against shoe retailer DSW was also dismissed when the court ruled that an increased risk of identity theft, by itself, is insufficient for conferral of standing. Data Security Handbook 122-123 (American Bar Association, Section of Antitrust Law 2008) (citing Key v. DSW, Inc., 454 F. Supp. 2d 684 (S.D. Ohio 2006).
17. Data Security Handbook 122-123 (American Bar Association, Section of Antitrust Law 2008).
18. *See* PCI Security Standards Council, PCI Data Security Standard, available at *https://www.pcisecuritystandards.org/index.shtml*; "TJX to pay $24M More for Lost Data," *USA Today*, Apr. 2, 2008, available at *http://www.usatoday.com/tech/techinvestor/industry/2008-04-02-tjx-data-breach_N.htm* (accessed Apr. 29, 2009).
19. Council Directive No. 95/46/EC, O.J. L. 281/31 (1995) (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data) (hereinafter, the Directive).
20. Brian Hengesbaugh, Michael S. Mensik, Lothar Determann, "Global Data Transfers and the European Directive: A Practical Analysis of the New ICC Contract Clauses," 4 *PVLR* 153.
21. The Directive defines "controller" to mean "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law." Directive at 38.
22. Commission Decision No. 2002/16/EC, O.J. L. 6/52 (2002) (Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC); Commission Decision No. 2004/915/EC, O.C. L. 385/74 (2004) (Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries).

23. *See* US/EU Safe Harbor Web site, *http://www.export.gov/safeharbor/*.
24. *See* the US/EU Safe Harbor privacy principles, available at *http://www.export.gov/safeharbor/eg_main_018247.asp*.
25. The Directive defines "processor" to mean "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller." Directive at 38.
26. Commission Decision No. 2002/16/EC, O.J. L. 6/52 (2002) at 58; Commission Decision No. 2004/915/EC, O.C. L. 385/74 (2004) at 78.
27. Commission Decision No. 2002/16/EC, O.J. L. 6/52 (2002) at 60; Commission Decision No. 2004/915/EC, O.C. L. 385/74 (2004) at 80.
28. German Federal Data Protection Act § 9, available at *http://bundesrecht.juris.de/bdsg_1990/anlage_73.html* (last visited July 3, 2009); *see* M. Schmidl, "The different facets of IT-security law," *BNA World Data Protection Report* 8 (2009).
29. *See* Royal Decree 1720/2007, §§ 79-114, available in English at *https://www.agpd.es/portalweb/english_resources/common/reglamentolopd_en.pdf* (last visited July 3, 2009).
30. Companies must change passwords every 90 days to protect sensitive data, otherwise, every 180 days. *See* Italian Data Protection Act, Arts. 31-35 and Annex B § 5 available at *http://www.privacy.it/privacycode-en.html* (last visited July 3, 2009).
31. *See* Cal. Civ. Code § 1798.82; *see also* Cal. Civ. Code § 1798.29.
32. *See* S.C. Code § 39-1-90, available at *http://www.scstatehouse.gov/code/t39c001.htm*.
33. *See* Alaska Stat. § 45.48.010, *et seq.*, available at *http://www.legis.state.ak.us/PDF/25/Bills/HB0065Z.PDF.*
34. National Conference of State Legislatures, State Security Breach Notification Laws, available at *http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx*.
35. *See* Tex. 81(R), H.B. 2004 available at *http://www.capitol.state.tx.us/tlodocs/81R/billtext/html/HB02004F.htm*.
36. *But see, e.g.,* Ark. Code § 4-110-101, *et seq.*, Cal. Civ. Code § 1798.82.
37. *See* Me. L.D. 970, available at *http://www.mainelegislature.org/legis/bills/bills_124th/chapters/PUBLIC161.asp.*
38. Cal. S.B. 20, available at *http://info.sen.ca.gov/pub/09-10/bill/sen/sb_0001-0050/sb_20_bill_20081201_introduced.html*.
39. *See* N.Y. Senate Open Legislation Service memo on N.Y. S3760, available at *http://open.nysenate.gov/openleg/api/html/bill/S3760*.
40. Minn. Stat. § 325E.64, available at *https://www.revisor.leg.state.mn.us/statutes/?id=325E.64*.
41. Minn. Session Laws, Regular Session, 2007, *https://www.revisor.leg.state.mn.us/laws/?doctype=Chapter&year=2007&type=0&id=108*.
42. *See, e.g.*, PGP Blogs, Just Who Should Pay for Data Breaches … and How? (Oct. 4, 2008), *http://blog.pgp.com/index.php/tag/plastic-card-security-act/* (last visited July 7, 2009).
43. Christine Mumford, "Industry Data Security Guidance, Not New Laws, May Be Best Path," 8 *PVLR* 462 (Mar. 23, 2009).
44. Cal. Civ. Code § 1798.81.5(b) (emphasis added). *See also* Cal. Civ. Code § 1798.81.5(d) (defining personal information); Cal. Civ. Code § 1798.81.5(a) (defining "owns or licenses"); Cal. Civ. Code § 1798.80 (defining "business").
45. Nev. Rev. Stat. § 603A.210(1) (emphasis added). *See also* Nevada Revised Statutes § 603A.030 (defining "data collector"); Nevada Revised Statutes § 603A.040 (defining "personal information").
46. *See* California Office Information Security & Privacy Protection, *http://www.oispp.ca.gov/*.
47. *See* Nevada Bureau of Consumer Protection, *http://ag.state.nv.us/idtheft/idtheft.htm*.
48. *See* Cal. Civ. Code § 1798.81.5(c); Nev. Rev. Stat. § 603A.210(2).
49. *See* Cal. Civ. Code § 1798.81.
50. *See* Cal. Civ. Code § 1798.85(a)(3). Unlike Nevada, California does not define "encryption."
51. Nev. Rev. Stat. § 597.970; *see also* Nev. Rev. Stat. § 205.4742 (defining "encryption broadly to be the "use of *any* protective or disruptive measure, including, without limitation, cryptography, enciphering, encoding or a computer contaminant, to: (1) Prevent, impede, delay or disrupt access to any data, information, image, program, signal or sound; (2) Cause or make any data, information, image, program, signal or sound unintelligible or unusable; or (3) Prevent, impede, delay or disrupt the normal operation or use of any component, device, equipment, system or network. (Emphasis added.)).
52. Nev. Rev. Stat. § 603A.220.
53. Or. Rev. Stat. § 646A.622, available at *http://www.leg.state.or.us/ors/646a.html*.
54. Or. Rev. Stat. § 646A.622(2)(b).
55. Or. Rev. Stat. § 646A.622(2)(c).
56. Or. Rev. Stat. § 646A.622(2)(a).
57. Or. Rev. Stat. § 646A.622(2)(d).
58. 201 CMR § 17.00, *et seq.*, as amended on Feb. 12, 2009, available at *http://www.mass.gov/Eoca/docs/idtheft/201CMR17amended.pdf* (hereinafter, the Massachusetts Regulations).
59. *See* Mass. Gen. Laws ch. 93H, available at *http://www.mass.gov/legis/laws/mgl/gl-93h-toc.htm*.
60. "Patrick Administration Issues Comprehensive Identity Theft Prevention Regulations & Executive Order," Consumer Affairs and Business Regulation, Press Release, Sept. 22, 2008, available at *http://www.mass.gov/?pageID=ocapressrelease&L=3&L0=Home&L1=Consumer&L2=Identity+Theft&sid=Eoca&b=pressrelease&f=080922_IDTheft_regsandexecorder&csid=Eoca*.
61. "Office of Consumer Affairs Files Revised ID Theft Regulations," Consumer Affairs and Business Regulation, Press Release, Feb. 12, 2009, available at *http://www.mass.gov/?pageID=ocapressrelease&L=1&L0=Home&sid=Eoca&b=pressrelease&f=20090212_idtheft&csid=Eoca*.
62. Massachusetts Regulations § 17.01(2).
63. Massachusetts Regulations § 17.02.
64. Massachusetts Regulations § 17.05.
65. Massachusetts Regulations § 17.02.
66. Massachusetts Regulations § 17.02.

67. Massachusetts Regulations § 17.03(1).
68. Massachusetts Regulations § 17.02.
69. Massachusetts Regulations § 17.03(2).
70. Massachusetts Regulations § 17.03(3).
71. Massachusetts Regulations § 17.03(4).
72. *See* Massachusetts Regulations § 17.02 (defining "encrypted" to be "the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation by the Office of Consumer Affairs and Business Regulation").
73. *See* Frequently Asked Questions Regarding 201 CMR 17.00, Office of Consumer Affairs & Business Regulation, available at *http://www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf*.
74. *Id*.
75. *Id*.
76. "Business Community Given Additional Time to Comply with Identity Theft Prevention Regulations," Consumer Affairs and Business Regulation, Press Release, Nov. 14, 2008, available at *http://www.mass.gov?pageID=ocapressrelease&L=1&L0=Home&sid=Eoca&b=pressrelease&f=081114_IDTheftupdate&csid=Eoca*.
77. "Office of Consumer Affairs Files Revised ID Theft Regulations," Consumer Affairs and Business Regulation, Press Release, Feb. 12, 2009, available at *http://www.mass.gov/?pageID=ocapressrelease&L=1&L0=Home&sid=Eoca&b=pressrelease&f=20090212_idtheft&csid=Eoca*.
78. Mass. S.B. 173, available at *http://www.mass.gov/legis/bills/senate/186/st00pdf/st00173.pdf*.
79. *See* Mass. Gen. Laws ch. 93H, available at *http://www.mass.gov/legis/laws/mgl/gl-93h-toc.htm*.
80. Nev. Rev. Stat. § 603A.210. *See also* Nev. Rev. Stat. § 603A.030 (defining "data collector"); Nev. Rev. Stat. § 603A.040 (defining "personal information).
81. Governor Jim Gibbons, Press Release, May 30, 2009, available at *http://gov.state.nv.us/PressReleases/2009/2009-05-30_BillSignedAdvisory.htm*.
82. Nev. S.B. 227, available at *http://www.leg.state.nv.us/75th2009/Bills/SB/SB227_EN.pdf*.
83. "Data storage devices" are defined broadly as any device that stores information or data from any electronic or optical medium and the medium itself," which includes computers and cellular telephones.
84. Nev. Rev. Stat. § 597.970.
85. Massachusetts Regulations § 17.01(2).
86. Christine Mumford, "Industry Data Security Guidance, Not New Laws, May Be Best Path," 8 *PVLR* 462 (Mar. 23, 2009).
87. Incidentally, New York has also defined its "encryption" requirements with respect to technology adopted by a standards setting body in proposed amendments to its security breach notification law. *See* N.Y. Senate Open Legislation Service memo on N.Y. S3760, available at *http://open.nysenate.gov/openleg/api/html/bill/S3760*.
88. This dual requirement may be the trend of stricter encryption requirements for data that is either in storage or in transit. Michigan's Senate Bill 1022 (2008) will mandate encryption of consumer data in storage "in conformity with industry-standard encryption methods and capabilities." *See* Mich. S.B. 1022 (2008). *http://www.legislature.mi.gov/(S(huy2gbrzieumzdjdl1n0cfyg))/mileg.aspx?page=getObject&objectName=2008-SB-1022*. Two pending bills in Washington, Substitute House Bill 2838 and Senate Bill 6425, would also require businesses to effectively encrypt personal information while they are either in storage or in transmission (by reference to the PCI DSS). *See* Wash. H.B. 2838, available at *http://apps.leg.wa.gov/billinfo/summary.aspx?bill=2838&year=2007#history*; Wash. S.B. 6425, available at *http://apps.leg.wa.gov/billinfo/summary.aspx?bill=6425&year=2007*.
89. *See* Massachusetts Regulations § 17.02 (defining "encrypted" to be "the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation by the Office of Consumer Affairs and Business Regulation").
90. Lothar Determann and Lars Brauer, "Employee Monitoring Technologies and Data Privacy—No One-Size-Fits-All Globally," 9 *IAPP Privacy Advisor* 1 (2009); Lothar Determann, "When No Really Means No: Consent Requirements for Workplace Monitoring," 8 *Electronic Commerce & Law* 892 (2003), republished in 4 *Privacy Officers Advisor* 10 (2003) and 3 *World Data Protection Report* 22 (2003).

Reprinted from *The Computer & Internet Lawyer*, September 2009, Volume 26, Number 9, pages 6 to 17, with permission from Aspen Publishers, Inc., a Wolters Kluwer business, New York, NY, 1-800-638-8437, *www.aspenpublishers.com*.