

Update On Mandating Data Security

By Andrew S. Ehmke¹ and Gavin D. George²

Many states have enacted statutes imposing general obligations on companies to maintain “reasonable” security procedures and practices to protect the personal information of state residents from unauthorized access or use.³ A few states, however, are taking data security statutes a step further by mandating that companies take specific actions to prevent a security breach. Nevada and Connecticut have imposed, and Massachusetts is about to impose, obligations on companies to comply with certain security measures when storing, transmitting and disposing of personal information. Companies with nationwide clientele, or employees located throughout the country, should be aware of the growing and varying data security requirements and should review their data protection programs to ensure that they are in compliance with developing requirements. This article explores a few specific developments in state law.

I. Massachusetts

Massachusetts enacted a data protection statute on October 31, 2007, authorizing the Massachusetts Office of Consumer Affairs and Business Regulation (“OCABR”) to develop data protection regulations.⁴ OCABR has now issued regulations set to go into effect on January 1, 2010. These regulations require companies, regardless of location, to comply with certain administrative and computer security requirements when storing or transferring the personal information of Massachusetts residents.

A. **Applicability**

The OCABR regulations apply to any company that “owns, licenses, stores or maintains personal information” about a Massachusetts resident. The reach of the regulations appears to cover data acquired from a customer, third party information vendors, and a company’s own employees. The OCABR regulations define “personal information” as any combination of a resident’s name and one of the following: Social Security number, driver’s license number, state-issued identification card number, or financial account, credit card, or debit card number.⁵ The regulations mandate that companies must comply with two types of requirements: (1) administrative requirements related to structuring an information security program, and (2) computer security requirements to implement the security program.

¹ Andrew S. Ehmke is a partner in the Intellectual Property Practice Group of Haynes and Boone. The focus of his practice is on intellectual property portfolio development, management, licensing, and commercialization. He may be reached at andrew.ehmke@haynesboone.com or 214.651.5116.

² Gavin D. George is an associate in the Intellectual Property Practice Group of Haynes and Boone. His practice focuses on intellectual property development and licensing. He may be reached at gavin.george@haynesboone.com or 214.651.5148.

³ e.g. CAL. CIV. CODE § 1798.81.5 (2004).

⁴ M.G.L.A. 93H § 6.

⁵ 201 C.M.R. 17.02.

B. Administrative Requirements

The OCABR regulations require affected companies to develop and implement a written security program, which must be consistent with industry standards and any applicable state or federal regulations.⁶ The regulations extend to credit, debit and card numbers even if stored without an associated security code, access code, or personal identification number. The Massachusetts regulations are applicable to both paper and electronic records.⁷

The security program must include, among other things:

- assignment of personnel to oversee and update the security program;
- identification of all records containing personal information;
- identification of security risks to records containing personal information;
- development of safeguards against security risks to records containing personal information;
- policies concerning physical and electronic access, storage, and transportation of records;
- employee training on the security program;
- disciplinary measures for security program violations by employees;
- oversight protocols for third-party service providers who may have access to personal information;
- measures to prevent terminated employees from accessing records containing personal information; and
- annual reviews of the security measures in place.⁸

C. Computer Security Requirements

The OCABR regulations also require certain technological standards to be met by the affected companies. Under the regulations, affected companies must employ:

- user authentication security protocols;
- restrictions and controls over access to personal information (such as password controls and multiple login failure lockouts);
- monitoring of data systems for unauthorized exposure of personal information;
- installation and updating of computer firewall and security software;
- encryption of records being transmitted wirelessly or across public networks; and
- encryption of personal information stored on laptops or other portable devices.⁹

⁶ 201 C.M.R. 17.01(c)(2).

⁷ 201 C.M.R. 17.02.

⁸ 201 C.M.R. 17.03.

⁹ 201 C.M.R. 17.04.

The regulations define “encrypted” as 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.”¹⁰

D. Penalties

Violations of the Massachusetts data protection statute carry a civil penalty of not more than \$5,000. In addition, the Massachusetts Attorney General may bring an enforcement action under the statute, which permits the imposition of injunctive relief and attorneys’ fees. Lastly, private civil lawsuits are available to Massachusetts consumers seeking damages under the data protection statute, which in certain instances, could be trebled.

E. Proposed Amendment

Massachusetts Senate Bill 173, if passed, may cause OCABR to curtail or dilute the data security regulations currently set to go into effect.¹¹ Senate Bill 173 proposes to (i) exempt certain companies from the requirements of the data protection statute if a federal data protection statute is applicable those companies, and (ii) eliminate any mandate to use specific technology or technologies, or a specific method for protecting personal information. It is not clear, however, whether the pending legislation completely overrides OCABR’s security regulations or simply prohibits OCABR from specifying particular technology to be used for data security.

II. Nevada

Nevada enacted a data security law on October 1, 2008, requiring that personal information of a customer must be encrypted by companies prior to transmission.

A. Applicability

The law states:

“A business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.”¹²

The statute does not define what constitutes a “business in this State.” Nor does the statute indicate whether the terms “customer” and “personal information”¹³ in the statute are limited to Nevada residents. Accordingly, as least on its face, the Nevada law appears very broad.

B. Computer Security Requirements

The Nevada statute requires encryption to ensure the security of electronic transmissions. “Encryption” is defined broadly, allowing companies some leeway in adopting a proper compliance program:

“The use of any protective or disruptive measure, including, without limitation, cryptography, enciphering, encoding or a computer contaminant, to:

¹⁰ 201 C.M.R. 17.02.

¹¹ <http://www.mass.gov/legis/bills/senate/186/st00pdf/st00173.pdf>

¹² NEV. REV. STAT. § 597.970 (2008).

¹³ NEV. REV. STAT. § 603A.040 (2008).

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.”¹⁴

C. Penalties

The penalties under the Nevada statute are not specified; which seems to indicate that civil liability will rest with the court system (perhaps under a negligence standard). Criminal penalties may also be possible, since Nevada law states that a violation of any statute without a specified penalty constitutes a misdemeanor.¹⁵ Misdemeanors in Nevada can result in up to six months of jail time and a fine of up to \$1,000.¹⁶

III. Connecticut

On October 1, 2008, Connecticut adopted a law that mandates certain security requirements regarding electronically stored personal information.

A. Applicability

The Connecticut statute reads:

“[a]ny person in possession of personal information of another person shall safeguard the data, computer files and documents containing the information from misuse by third parties, and shall destroy, erase or make unreadable such data, computer files and documents prior to disposal.”¹⁷

By covering “any” person with personal information, the Connecticut law expansively appears to cover businesses storing customer information, government entities, and employers. “Personal information” is also broad in scope, and is defined as “information capable of being associated with a particular individual through one or more identifiers.”¹⁸ Moreover, the law does not limit the scope of “personal information” to Connecticut residents. Therefore, the law appears to cover both Connecticut businesses storing personal information about other states’ residents, as well as businesses located in other states storing personal information of Connecticut residents.

B. Computer Security Requirements

The Connecticut statute requires not only safeguarding personal information when a company electronically transfers such information, but also requires erasure or destruction of personal information when a company disposes of such information. The Connecticut law also requires companies to “create a privacy protection policy which shall be published or publicly displayed...

¹⁴ NEV. REV. STAT. § 205.4742 (2008).

¹⁵ NEV. REV. STAT. § 193.170 (2008).

¹⁶ NEV. REV. STAT. § 193.150 (2008).

¹⁷ 2008 Conn. Pub. Acts 08-167, Section 1(a).

¹⁸ 2008 Conn. Pub. Acts 08-167, Section 1(c).

on an Internet web page” and to “[p]rotect the confidentiality of... prohibit unlawful disclosure of... and limit access to Social Security numbers.”¹⁹

C. Penalties

The Connecticut statute mandates a civil penalty of \$500 for each violation, up to a maximum penalty of \$500,000 per individual event.

IV. Compliance with Data Security Laws

In the future, it is likely that additional states will require companies to implement data security measures with varying degrees of specificity and with varying requirements. For example, legislation is pending in Michigan and Washington that would require companies to encrypt stored personal data. Companies that adopt a comprehensive program that complies with existing and anticipated state and federal regulation of personal data will minimize the chance of incurring statutory penalties, as well as costly data breaches. Companies with national clientele or employees should be especially aware of the ever-growing number of state data security requirements. Given the scope of some of the administrative and computer security controls imposed by state law, companies are advised to review their data protection programs frequently to ensure compliance with the ever-evolving landscape.

¹⁹ *Id.*