Stay Current.

October 2004

California Creates New Affirmative Data Security Duty

By Michael K. Lindsey and John R. Sabatini

Late last month, California Governor Arnold Schwarzenegger signed into law Assembly Bill 1950 (the "Act"), which requires certain businesses to implement and maintain "reasonable" security measures to protect personal data about California residents. The law also requires affected businesses to enter into agreements with any business partners who have access to such information, requiring that those businesses adopt reasonable security measures. The Act will be added to the California Civil Code as section 1798.81.5 and provides for remedies that include injunctive relief and recovery of actual damages.

Purpose of the Act

The Act is designed to supplement existing state privacy-protection laws that have been enacted in recent years by articulating a standard as to how businesses must maintain personal information on an ongoing basis. Earlier enactments provided that businesses must destroy consumers' personal information that they no longer intend to retain and that businesses must notify consumers in the event of data security breaches.[1] Another recent California law specifies that businesses with Internet sites which collect personal information about California residents must adopt and conspicuously post privacy policies, without specifying the expected substance of such policies.[2] The prior legislation stopped short of mandating a particular standard of care, which the Act now provides.

Who is Covered By the Act?

Any businesses that "own or license" personal information about California residents must adhere to the standard set by the Act. The Act does not define the term "own or license," but it does expressly provide that the term is intended to encompass businesses that retain or use personal information in connection with maintaining internal customer accounts or completing transactions with customers. Presumably, the Act is intended to reach any business, wherever located, that maintains personal information concerning any California consumer as part of its business activities.

The Act expressly does not apply to certain types of businesses that are subject to other privacy laws. More specifically, the Act does not apply to (i) healthcare providers subject to the Confidentiality of Medical Information Act or Health Insurance Portability and Availability Act of 1996 (HIPAA); (ii) financial institutions subject to the California Financial Information Privacy Act; (iii) entities that obtain information subject to the confidentiality provisions of the Vehicle Code; or (iv) businesses that are regulated by federal or state laws providing even greater protection to personal information than the Act.

What Information is Covered By the Act?

The personal information protected by the Act includes a resident's first name or initial and last name, in combination with one or more of the following: (i) social security number; (ii) driver's license; (iii) account number, credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account; or (iv) medical information – i.e., individually identifiable information about an individual's medial history, medical treatment or diagnosis by a health care professional. The Act extends to such information only if the name or data elements are unencrypted or unredacted. On its face, the Act does not require any particular type or level of encryption, although, if experience under similar prior California laws is a guide, California regulators at the Office of Privacy Protection soon may attempt to fill that perceived gap. In addition, the Act does not apply to information that is lawfully made available to the public from federal, state or local government records.

What Standard of Care Does the Act Require?

Businesses subject to the Act must implement and maintain "reasonable security procedures and practices appropriate to the nature of the information" to protect the information from unauthorized access, destruction, use, modification or disclosure. The Act does not specify the nature or degree of security measures that must be implemented, apparently leaving that for courts and standard-setting organizations to define. In any event, security measures that may be sufficient for some kinds of information and some kinds of businesses may not be sufficient for others. Further, security standards may evolve over time, particularly in connection with advances in technology.

In addition, businesses that disclose personal information about California residents to their nonaffiliated business partners must require those partners to implement their own reasonable safeguards. The Act does not necessarily require that a business impose its particular security standards on its partners, but both parties must satisfy the reasonableness standard set by the Act, as measured against the particular information at issue.

What Are the Penalties for Violating the Act?

By reason of the Act's incorporation into Title 1.81 of the California Civil Code, consumer remedies for violations of the Act can include injunctive relief and recovery of actual damages. Importantly, neither the Act nor Title 1.81 prohibit class actions.

Conclusion

But for the governor's veto, two additional privacy bills would have been adopted in California this year. Senate Bill 1451 would have made any person, wherever located, who violates the privacy of a California resident's personal information subject to legal action in California. Senate Bill 1841 would have prohibited employers from electronically monitoring employees without notice about the nature and purpose of the monitoring. California continues to live up to its reputation as the most active U.S. forum for legislation in the fields of data privacy and security.

Notes

1. See "Client Alert: New California Law Requires Notification of Security Breaches Involving Personal Information" (http://www.paulhastings.com/media/news/media.177.pdf) and "Stay Current: Interpreting California's Data Security Breach Notification Law: Best Practice Recommendations Issued by the Office of Privacy Protection" (http://10.5.5.89/media/news/media.319.pdf), which concern the notice requirement in the event of data security breaches pursuant to Cal. Civ. Code §§ 1798.82, *et seq.*, and include recommendations for data security that apply with equal force under the Act.

2. See "Stay Current: California Enacts Nation's First State Online Privacy Protection Act" (http://www.paulhastings.com/media/news/media.808.pdf), which concerns the Cal. Bus. & Prof. Code §§ 22575, *et seq.* requirement that website operators that collect California residents' personal information maintain and post privacy policies

If you have any questions about the Act or its application to your company's privacy practices, please contact the Paul Hastings attorney with whom you usually speak or any of the attorneys listed below:

Los Angeles
Michael K. Lindsey (213) 683-6262
michaellindsey@paulhastings.com

John R. Sabatini (213) 683-6179
johnsabatini@paulhastings.com

Washington, D.C.
Behnam Dayanim (202) 508-9564
bdayanim@paulhastings.com

New York
John J. Altorelli (212) 318-6607
johnaltorelli@paulhastings.com

Robert L. Sherman (212) 318-6037
robertsherman@paulhastings.com

Adam E. Kraidin (212) 318-6783
adamkraidin@paulhastings.com