

Privacy Newsletter

JULY 2003

www.mintz.com

New California Privacy Law Requires Disclosure of Security Breaches

On July 1, 2003, a new privacy law¹ took effect in California which may impact the way your company handles and stores personal information. While many privacy laws and pending privacy bills address the collection, use and dissemination of personal information, this law takes a different approach and addresses security breaches. Under the new law, a company that owns, licenses or maintains personal information of California residents may be required to notify those residents if a security breach enables an unauthorized person to acquire their unencrypted personal information. Due to the broad and sweeping nature of the legislation, all companies should consider the impact of the law on their security systems and internal procedures with respect to the handling of personal information.

Effect of the Law Outside of California

The California law affects any person or business that conducts business in California and owns, licenses or maintains computerized data that includes personal information of California residents. To understand if your business falls under this umbrella, first determine if you “conduct business in California.” Assume that this is a loose standard requiring only a minimal connection between your business and the state of California. Consider not only whether your company has a physical presence in California (which is not required to be conducting business there), but whether it makes sales in California, uses California suppliers or has contracts with California businesses. These are just a few examples of activities that might constitute “conducting business in California.”

Next, determine if your business owns, licenses or maintains personal information of California residents. You fall within this definition if you are a third-party service provider to the owner of the information, so take into account not only your own data, but that of your clients and customers if such data is on your systems. For purposes of this law, “personal information” means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (a) social security number, (b) driver’s license number or California Identification Card number, (c) 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. “California resident” includes, without limitation, your customers, clients, employees and investors.

Requirements of the Law

If the above factors indicate that your business is subject to the California law, be aware of your new obligations. The law requires that you disclose any breach of the security of a system containing unencrypted personal information of a California resident if the information was, or is reasonably believed to have been, acquired by an unauthorized person. Licensees and those who maintain personal information on behalf of an owner

(continued on page 2)

¹ Senate Bill No. 1386, to be added to the California Civil Code as Section 1798.29.

New California Privacy Law (continued from page 1)

must notify the owner of the personal information of the breach, and they may have an obligation to notify the residents as well. There is no specified time period for notification, but it must be as expeditious as possible and without delay. The law provides for several forms of notice, both written and electronic, subject to certain requirements. These requirements should be reviewed before issuing any notices in order to ensure compliance with the law. Penalties for failure to comply with the law are not specified, but rather are based on injury to the individual whose information was acquired. Any injured person can bring civil suit for a violation of the law, and class action lawsuits are not precluded.

Safe Harbor Provisions

The general intent of the law is to encourage security measures to protect the unauthorized disclosure of personal information. In keeping with that intent, the law provides a safe harbor for personal information that is encrypted.

If the personal information is encrypted, disclosure of a security breach is not required. However, the law does not define what “encrypted” means, nor does it set a standard for encryption. As a result, there is some ambiguity and uncertainty as to the extent of the safe harbor protection.

Compliance Recommendations

Given the broad scope and many ambiguities of this new law, compliance is as much an art as it is a science. However, there are certain affirmative steps companies can take towards compliance. First, to take advantage of the safe harbor for encrypted data, evaluate if there are means of encrypting personal information available on your systems or the systems of your vendors. Any level of encryption is an improvement over unencrypted data. Second, to the extent they are not already in place, implement procedures to prevent security breaches and monitor your systems, and ensure that your staff and vendors are trained on such procedures. Finally, include in your security plan a provision that deals with the specific requirements to notify California residents as expeditiously as possible and without delay if the security of their personal information has been, or may have been, breached.

The California law is likely to serve as a model for additional legislation in other states as well as at the federal level. Even if you are not currently subject to the law, it is worth paying attention to with an eye towards future developments in this area. ○

MINTZ LEVIN
COHN FERRIS
GLOVSKY AND
POPEO PC

ML
STRATEGIES

Mintz Levin and ML Strategies provide legal, legislative and consulting expertise on privacy as it relates to many issues. If you would like further information, please contact the Mintz Levin attorney who regularly handles your legal affairs, or one of the attorneys or senior professionals listed below.

Privacy Regulation

Neil H. Aronson.....	617 348 1809
John M. Delehanty.....	212 692 6703
Robert Duggan	617 348 1780
Christopher J. Harvie	202 434 7377
Laura A. Huber	617 348 1856
Paul A. Hughes	203 787 6320
Julie E. Korostoff.....	617 348 1638
Fernando R. Laguarda	202 434 7347
Cynthia J. Larose	617 348 1732
Frank J. Marco.....	203 787 6310
Susan E. McDonald	202 434 7397
Bruce D. Sokler	202 434 7303
Howard J. Symons	202 434 7305
Ivan S. Wool.....	212 692 6757
Wayne M. Zell	703 464 8135

Health Privacy

Michael D. Bell	202 434 7481
Linda D. Bentley	617 348 1784
Susan W. Berson	202 661 8715/212 692 6750
Raymond D. Cotton.....	202 434 7322
Erin Lewis Darling.....	202 434 7478
Hope S. Foster	202 661 8758
Ellen L. Janos.....	617 348 1662
Peter M. Kazon	202 661 8739
Rebecca A. Matthews	203 787 6329
M. Daria Niewenhous	617 348 4865

Privacy Litigation

Michael S. Gardener.....	617 348 1642
Kevin M. McGinty	617 348 1688
Laurence A. Schoen	617 348 1764

Employment Privacy

Jennifer B. Rubin	203 787 6324/212 856 8960
-------------------------	---------------------------

Legislative Privacy Strategies

David J. Leiter	202 434 7346
-----------------------	--------------

Public Relations Strategies

Jason D. Glashow	617 348 1667
------------------------	--------------