

NEW CALIFORNIA LAWS REGARDING DIRECT MARKETING, COMPUTER SPYWARE, PERSONAL INFORMATION SECURITY AND PROTECTION OF SOCIAL SECURITY NUMBERS

By Stephen H. LaCount, Esq.

Companies that disclose consumers' personal information for use in direct marketing campaigns will be required to meet certain obligations imposed by California's direct marketing disclosure statute due to take effect on January 1, 2005. In addition, Governor Arnold Schwarzenegger recently approved four additional laws further extending privacy protection in California. These laws address spyware, security obligations with respect to personal information, collection of medical information for direct marketing purposes, and protection of social security numbers.

Direct Marketing Disclosure Statute (Senate Bill 27 Takes Effect on January 1, 2005)

Personal Information. This statute requires a company to provide individual California customers, upon request, with certain information concerning disclosure of "personal information" to third parties during the prior calendar year. The statute purports to cover any company that has established a business relationship with California residents and clearly targets companies that disclose customers' personal information to third party marketers. For purposes of this statute, "personal information" is any information that identifies, describes or can be associated with an individual, and includes categories ranging from name, address, or email address to product purchases.

Disclosures to Third Parties. Any recipient of personal information that is a separate legal entity from the disclosing company is considered a "third party" under the statute. Accordingly, disclosures to affiliates are covered under the statute, although the requirements are reduced for affiliates that share the same brand name. [*The statute excludes specific types of business-related disclosures to third parties, such as disclosures to vendors used for data administration, marketing and customer service, provided that those third parties do not disclose or use the information for their own direct marketing purposes*].

Customer Definition. Companies are required to respond to requests by a "customer", defined by the statute as "a resident of California who provides personal information to a company pursuant to an established business relationship for personal, family or household purposes".

Types of Disclosure and Customer notification. The statute provides that a covered company must respond to requests for information about third party use of personal information and defines steps required to be taken to notify California customers of their ability to request this disclosure.

Consumer Protection Against Spyware Act (Senate Bill 1436 Takes Effect on January 1, 2005)

First Regulation of Spyware. The Consumer Protection Against Computer Spyware Act (“CPACSA”) represents California’s first regulation of spyware, and one of the first such anti-spyware laws in the country. The CPACSA makes it illegal for anyone to install software on another person’s computer...and willfully or in deliberately deceptive way to use it for wrongful purposes, such as modifying settings, collect personal information or take control over a computer to send commercial emails or viruses.

Narrowly Drawn Scope. Critics of the law have argued that it does not go far enough, as it requires “willful or intentional deceptive actions” to trigger a violation. Further, the Act does not prohibit spyware – and merely requires notification before the spyware is installed.

Security Requirements on Companies that Own or License Personal Information (Assembly Bill 1950 Takes Effect on January 1, 2005)

Reasonable Security Procedures and Practices. Companies that own or license *unencrypted* personal information must “implement and maintain reasonable security procedures and practices” for that data. The statute does not detail the level of security required but states that it must be “appropriate to the nature of the information to protect the personal information” from unauthorized access, destruction, use, modification or disclosure. Further, Companies subject to this law may only disclose such information to unaffiliated third parties who contractually agree to maintain reasonable security measures. [*Businesses that comply with stricter privacy laws such as health care providers and entities covered by Health Insurance Portability and Availability Act (“HIPPA”) are deemed to be in compliance with the California law*].

Personal Information. The statute defines “personal information” as including an individual’s name in combination with one or more of the following data elements, if either the name or data element is unencrypted or unredacted: (i) social security number, (ii) driver’s license or California identification card number, (iii) account number in combination security code or password, and (iv) medical information.

Collection of Medical Information For Direct Marketing Purposes (Senate Bill 1633 Takes Effect on January 1, 2005)

This law prohibits businesses from making a direct request to an individual for medical information for direct marketing purposes without first clearly informing the individual that the business intends to use the information to “market or advertise products, goods and services,” and obtaining the consent of the individual. Oral disclosures and consents must be recorded and maintained for two years and written disclosures must include a written consent. [*The law does not apply to health care plans, insurance companies or agents, and certain telephone companies*].

Displaying Social Security Numbers on Paychecks (Senate Bill 1618 Takes Effect on January 1, 2008)

This law amends the Labor Code with respect to disclosure of information displayed on itemized wage statements. Existing law in California requires employers to display on each pay stub the name of the employee and social security number. The new law dictates that employers shall display only the last four digits of an employee's social security number (or another employee identification number) on pay stubs or other checks, drafts or vouchers.