California Privacy Law Developments Alert

NEW CALIFORNIA LAWS REGARDING COMPUTER SECURITY BREACHES, ANTI-SPAM AND ONLINE PRIVACY PROTECTION

By Stephen H. LaCount, Esq.

Following on the heels of a 2002 privacy law which forced businesses to remove social security identifiers in an effort to combat identity theft, California has enacted three new laws which took effect in mid-2003, or will take effect in 2004. These ground breaking laws will significantly effect the way California and non-California businesses conduct their affairs with California residents. This client alert provides an overview of these laws, including mention of less restrictive federal legislation which may preempt certain provisions of these laws.

California Database Protection Act ("CDPA").

On July 1, 2003, a California law (new California Civil Code Section 1798.82 known as the California Database Protection Act) took effect that requires businesses to disclose to California residents any breach in the security of their computerized data if that breach would result in the acquisition of personal information by unauthorized users.

The CDPA was prompted by a much publicized computer intrusion into a California State government system that stored payroll information on 265,000 State Workers. Confidential data accessed included employee names and addresses, social security numbers, and bank information. The State did not become aware of the breach for some weeks and failed to timely report the intrusion to the affected employees. (Experts estimate that at least 100,000 security breaches occur every year). Efforts to curtail the proliferation of security breaches have intensified across the country, and federal legislation modeled after the CDPA was introduced by Senator Dianne Feinstein (D-CA) in late 2003.

CDPA requires any agency, person or business that owns or licenses computerized data which includes certain "personal information" of California residents to report any breach of the security of its computer system to the California residents whose *unencrypted* personal information was, or is reasonably believed to have been acquired by an unauthorized person. "Personal Information" is defined as an individual's first name or first initial, combined with the last name plus any one of a number of identifiers: (1) Social Security number; (2) driver's license number or California Identification Card number, or (3) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to the account. A security breach is defined as the "unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by a person, agency or business." Disclosure of a breach to affected California residents

must take place by either written notice or electronic notice "in the most expedient time possible and without unreasonable delay".
If a business fails to provide prompt notice to individuals following a security breach, the CDPA provides that any California resident injured by a violation may bring a civil action against the business to recover damages (courts are also empowered to grant injunctory relief).

California Anti-Spam Law and CAN-SPAM Act.

On September 23, 2003, California enacted into law (set to take effect on January 1, 2004) the toughest anti-spam legislation in the country (but certain provisions of this law will be supplanted by recently passed federal legislation). The California anti-spam law goes far beyond annoying bulk e-mails and broadly prohibits sending even a single e-mail advertisement or promotional message from California, or to a California e-mail address, unless the sender has first received the addressee's direct, *opt-in* consent to receive such messages.

The California anti-spam law bans more than just "spam" – all "unsolicited commercial e-mail advertisements" which are intended to promote or advertise goods and services are prohibited. The e-mail is "unsolicited" if it is sent to a recipient (1) with whom the sender does not have a pre-existing or current business relationship, and (2) who has not provided "direct consent" to receive this type of e-mail correspondence. The impact of the California law is such that companies would be required to reevaluate even commonplace uses of email for business development or promotional purposes.

CAN-SPAM Act. On December 8, 2003, Congress approved the long-awaited bill known as the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" or "CAN-SPAM Act" that creates a federal regime for the regulation of spam e-mail. (It is reported that President Bush has indicated his intention to sign the bill into law in the near future). The CAN-SPAM Act preempts existing state anti-spam laws, including the more restrictive California Anti-Spam Law, except to the extent that provisions of such state laws prohibit "falsity or deception" in any portion of an e-mail or attachment. Unlike the California anti-spam law which requires opt-in consent, the CAN-SPAM Act will permit the sending of unsolicited commercial email if recipients are provided a means to "opt out" of future mailings from senders. CAN-SPAM also prohibits certain fraudulent and misleading practices.

Unlike the California anti-spam law which would have given recipients the right to sue spammers, the CAN-SPAM Act authorizes only the Federal Trade Commission ("FTC") to bring enforcement proceedings against violators. The FTC is also empowered to establish a national "do not spam" list similar to the do not call registry that currently restricts telemarketing calls. CAN-SPAM requires the FTC to enact implementing rules within 12 months of the Act's effective date. The complex and extensive definitions and prohibitions contained in the federal legislation will no doubt raise a number of unresolved questions, and we will issue a subsequent client alert providing a more comprehensive treatment and analysis of the provisions of the CAN-SPAM Act.

California Online Privacy Protection Act ("OPPA")

In late 2003, California enacted its Online Privacy Protection Act which will take effect on July 1, 2004. OPPA requires all owners of commercial Internet websites or online services – referred to as "operators" – that collect personally identifiable information (e.g., first and last name, home or other physical address, an e-mail address, telephone number, social security number) from California residents to "conspicuously post" their privacy policies on their websites. Among other elements, the privacy policies must state the categories of personally identifiable information that operators collect from consumers and must identify the types of third parties with whom that information will be shared.

A privacy policy is considered conspicuously posted if any of these means are used: (1) the actual policy is displayed on the operator's home page; (2) an icon hyperlinked to the actual privacy policy contains the word "privacy" and uses a color that contrasts with the background of the web page ; or (3) hypertext linking the privacy policy to the home page includes the word "privacy" and is written in capital letters equal to or greater in size than the surrounding text, or is otherwise readily distinguishable from the surrounding text on the home page. Operators will be considered in violation of the Act upon failure to post their privacy policy within thirty (30) days after being notified of their noncompliance.

The new OPPA law does contain its own enforcement provisions. It is expected that OPPA will be enforced through California's Unfair Competition Law ("UCL"), which is incorporated in the California Business and Professions Code Sections 17200-17209. Under the UCL, the Attorney General, district attorneys, and certain county and city attorneys may bring civil actions seeking civil penalties and injunctive or other equitable relief. Of greater concern, however, is the potential for frivolous litigation brought under the "private attorney" provision of the UCL which permits persons who have suffered no harm to bring a private action for restitution or injunctive relief - and recover attorney's fees.