

## **New Laws Attempt to Regulate the Internet**

### **By Scott Hervey**

Last year the Internet was front and center in a number of controversies and new legislation. Aside from the music and movie industries continuing struggle and court battles over content piracy, 2003 saw significant legislative activity in areas dealing with the Internet. California's legislators spent a significant amount of time on Internet related legislation, including crafting extremely strong anti-spam laws (SB 186) only to have it preempted by a weaker Federal act. What follows below is a wrap up of the more relevant Internet legislation, Federal and State, passed last year.

### **THE FEDERAL CANSPAM ACT**

In the early days of December, 2003, the United States Congress enacted the Controlling the Assault of Non Solicited Pornography and Marketing Act of 2003, also known as the CANSPAM Act of 2003. Supporters of this act call it tough; it has substantial criminal penalties and fines for spammers. The chief co-sponsor of the Act, Senator Charles Schumer (D-New York), is quoted as saying: "With this bill, congress is saying that if you are a spammer you can wind up in the slammer." However, critics of the Act, which goes into effect January 1, 2004, complain that it does not go far enough and is not as tough as its supporters would like the general public to believe.

CANSPAM prohibits specific conduct related to electronic mail. Specifically, the Act prohibits the use of false headers, using false information to register five or more email accounts and intentionally initiating multiple commercial email messages from any combination of these accounts; engaging in email address harvesting and "dictionary attacks"; using scripts or automated programs to register multiple electronic mail accounts for the purpose of transmitting commercial electronic mail messages; and relaying or retransmitting commercial electronic mail messages through a computer network which the person does not have access rights, as well as other tricks of the spam trade. The Act provides for substantial monetary fines and penalties as well as jail time up to five years. In addition, the Act provides for forfeiture of all property traceable to the gross proceeds obtained from the offenses, and any equipment or other technology used in committing the offenses.

The Act also requires the senders of sexually oriented material to place a warning label on commercial electronic mail that contains sexually oriented material. However, if the recipient of these messages has already provided his or her affirmative consent to continue to receive these messages, no warning label is required.

While the imposition of civil fines, forfeiture and jail time make the Act sound rather ominous, critics still complain it will not stem the flow of spam. Critics say the problem is that the new law lacks an opt-in mechanism. This, critics say, will allow

spammers to continue to send unwanted spam, despite the Act's harsh criminal and civil penalties, as long as the message contains an opt-out mechanism and a functioning return email address. Because the new federal law preempts state law that specifically regulates commercial email messages, provisions like California's law which requires express consent or a prior commercial relationship will not apply.

The new federal law places enforcement with the Federal Trade Commission and allows civil actions by the various state Attorney General Offices. The Act also allows a limited private cause of action by internet access service providers. However, unlike California's law, the new federal law does not provide a private cause of action by consumers. Still, most commentators believe that California consumers will be able to pursue a remedy under California's unfair competition laws. (Business and Professions Code section 17200)

The preemption provision does leave some exceptions. The Act only supersedes state law that "expressly regulates the use of electronic mail to send commercial messages except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto." In addition it appears that states may still have the right to pursue claims that may arise in spamming situations, such as state trespass laws, breach of terms of service or use contracts, and actions under the Computer Fraud and Abuse Act.

On an international level, the new federal act places the United States at odds with Europe and its spamming legislation. In Europe, for the most part, spam is per se illegal. 90% of Europe's spam originates in the United States where spamming, after January 1, 2004, will be allowed. This is bound to cause tension between the United States and Europe as the two nations continue to attempt to harmonize intellectual property laws.

Outspoken critics of spam lament that the new federal law will do absolutely nothing to stem the growing tide of unwanted commercial email. Some critics note that spammers are deceptive by nature and, despite the new law, would not hesitate to use false or misleading email headers. In addition, the Act will do nothing to prevent serious spammers from opening up accounts in Bermuda or South Africa and continue to bombard the United States with spam from off shore.

## **COMPANIES NOW REQUIRED TO DISCLOSE BREACHES OF DATABASE SECURITY**

Beginning July 1, 2003, a new law will require businesses to disclose to California residents any breach in the security of their databases when that breach results in or could reasonably result in the disclosure or acquisition by an unauthorized third party of personal information about California residents. This also applies to companies that maintain computerized data for others .

This new law enacts California Civil Code section 1798.82 which applies to companies located both within and outside of California. While the new law was implemented as a measure to combat the increasing incidents of identity theft, it will also have sweeping implications for a wide range of businesses. While companies that encrypt all personal data will be exempt from the new law's disclosure requirements, those that do not must begin to comply with the law or face penalties prescribed in the statute.

The new Civil Code section 1798.82 revolves around the unintended disclosure or acquisition of "personal information" due to a breach in the security of a computer database. The statute provides: "Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." The section also provides that "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

A breach of the security of the system occurs when there is an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. The Good faith acquisition of personal information by an employee or agent of the owner of the system for business purposes is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

The type of personal information which triggers the disclosure requirement includes an individual's first name or first initial and last name in combination with any one or more of the following:

- (1) Social security number.
- (2) Driver's license number or California Identification Card number.
- (3) 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.

Not included in the definition of "personal information" is publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Upon discovery of a breach in the security of a business database, the business must notify California residents of the breach in "the most expedient time possible and without unreasonable delay." Business may make these notifications through written notice. A business may also make these notices electronically, as long as the notice provided is

consistent with the provisions regarding electronic records and signatures as provided in the Electronic Signatures in Global and National Commerce Act.

If the business required to provide notice to Californians regarding the breach of security can demonstrate that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the business must send out more than 500,000 notices, or that the business does not have sufficient contact information the business may provide substitute notice through e-mail notice, posting the notice on the businesses web site, and notification to major statewide media.

The new law applies to companies that conduct business in California, regardless of whether they are located physically within the state. The statute gives no guidance on the circumstances when a company is conducting business in California, and therefore subject to the provisions of the statute. This lack of guidance makes it extremely difficult for companies not domiciled in California to determine whether they must comply.

If an out of state company is subject to the provisions of the statute and does not know it, that company could be in for a rude awakening. The statute authorizes any customer injured by a violation of the statute to recover damages.

If they haven't already done so, companies should take steps to comply with the new law. Companies should establish internal policies and protocols that would be implemented when a breach which would require notice under the statute is discovered. In doing so, the company should implement a means to retain all records dealing with the discovery of the security breach and subsequent notification if it is later challenged in a civil suit.

## **CALIFORNIA ADOPTS AN ONLINE PRIVACY POLICY**

The California Online Privacy Protection Act of 2003 which goes into effect on July 1, 2004 requires the operator of a commercial website to maintain a privacy policy which meets certain requirements. The privacy policy must specifically provide the following information: 1) it must clearly identify the categories of personal user information (i.e., first and last name, street address, e-mail address, telephone number, Social Security number and any other information that would enable the user to be contacted either online or offline) collected through the website; 2) it must provide a a description of the process by which a user can review and request changes to any personal user information; 3) it must explain how the operator will notify consumers of changes to the privacy policy; and 4) and it must provide the effective date of the privacy policy. The Act requires the commercial operator to "conspicuously post" such a privacy policy.

To be conspicuously posted, the privacy policy must either be posted on the home page or there must be an iconic or text hyperlink on homepage or the first significant page that links to privacy policy. The icon or text hyperlink must contain the word "privacy"

and must be in a color an/or size which contrasts with the background and surrounding text.

The reach of the Act is longer than most might think. The new privacy policy requirements apply to operators of commercial websites or online services that collect personally identifiable information through a website from individual consumers who live in California, regardless where the website operator resides.

*Scott is a shareholder with Weintraub Genshlea Chediak Sproul. He is the immediate past chair and current vice chair of the California State Bar Cyberspace Law committee*