

# Privacy & Security Law Update

## California Privacy Laws Create Compliance Challenges

Privacy professionals are generally quite familiar with California's security breach notification law<sup>1</sup> as well as its counterpart AB 1950<sup>2</sup>,



which requires unregulated entities to protect sensitive personal information using reasonable security measures. But other California laws continue to generate compliance headaches for privacy officers.



### “Shine the Light”

California's Shine the Light law<sup>3</sup> is designed to help individuals understand corporate data sharing and opt-out of marketing. It requires many companies<sup>4</sup> doing business in California to respond to customer requests for information about disclosures of personal information to affiliates and third parties for marketing purposes.

Alternatively, companies can provide individuals with a mechanism to opt-out of all the data sharing.

If a company subject to the law has disclosed personal information about its California customers to a third party for marketing, it must inform customers of: (i) the categories of personal information that have been disclosed, (ii) the names and addresses of third parties

to whom they have been disclosed, and (iii) in some cases, the types of products that the third parties market.

The response may be limited if the company only discloses information to affiliates with same brand name and the information does not include: home telephone number; number, age or gender of children or the email or address of children; height, weight, race or religion; medical condition, drugs, therapies or products used; Social Security number; financial account or payment card numbers or balances.

If any of these data elements are shared, the company must generally inform its customers of the categories and provide the name and address of every recipient.

*continued on page 2*

### IN THE SPOTLIGHT... Wireless CAN SPAM

When testing your CAN SPAM compliance program, be sure to consider the Federal Communications Commission's rule regarding mobile service commercial messages (MSCMs). MSCMs are emails or SMS text messages to cell phones or other wireless devices.

Section 14(b)(1) of the CAN-SPAM Act required the FCC to provide wireless subscribers with the ability to avoid receiving MSCMs, unless they have expressly authorized the receipt of such messages. The FCC rule can be summarized as follows:

- The wireless subscriber must truly opt-in by taking an affirmative action. For example, if the authorization is collected online, the subscriber must check a box or click a button.

- Wireless subscribers must not bear any costs of authorizations or revocations. Revocations must be processed within 10 days.

- Each authorization must include disclosures that the subscriber: (1) is agreeing to receive MSCMs from a particular sender, (2) may be charged by the wireless provider to receive the messages, and (3) may revoke the authorization at any time.

- The authorization must clearly identify the entity that is being authorized to send the MSCMs. The authorization is personal as to the sender. Senders may not send MSCMs on behalf of other third parties, including affiliates.

This rule only applies to emails/SMS messages sent to devices with addresses in domains on the FCC's wireless domain name registry. It does not apply to emails that are merely forwarded to wireless devices, such as blackberries.

If you don't have an opt-in regime established, you can scrub the wireless domains from your email lists by downloading the registry at: <http://www.fcc.gov/cgb/policy/DomainNameDownload.html>.

**Privacy Studio.com**

The Art of Information Management

## California Laws

Covered companies must designate postal and email addresses to receive customer requests for information. They must answer requests to these addresses within 30 days. Requests received elsewhere must generally be answered within 150 days. The response can be standardized.

Shine the Light also requires each company to do one of the following:

- Train all managers of customer-facing employees on the designated addresses;
- Add a link on the company's website home page called "Your Privacy Rights" (or "Your California Privacy Rights") that describes their rights and provides the designated addresses; or
- Make the designated addresses available in each place of business in California where the company regularly has contact with customers.

### The Song-Beverly Credit Card Act

Lawsuit filings reveal that many retailers remain unaware of the Song-Beverly<sup>5</sup> data collection restrictions. A 1991 amendment to this Act specifically prohibits retailers from requiring or requesting personal information in connection with a credit card transaction.

The Act applies to *personal identification information*, which is "information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number."

This Act was tested in 2003 in the *Linens 'n Things* litigation.<sup>6</sup> In this case, the retailer asked consumers to voluntarily provide a phone number prior to making a purchase. In reinstating the case, the court noted that the Act seeks to prevent companies from combining different pieces of information to create a customer profile that can be used for marketing purposes. Prohibiting retailers from requesting personal information in conjunction with credit card use was necessary to effectuate the "obvious purpose" of the Act, preventing the matching of personal information with credit card numbers.

Retailers who ask for personal information – phone number or zip code – at point of sale are likely violating this law if the consumer then offers a credit card for payment. The fact that customers provide personal information voluntarily does not overcome the violation.

### Social Security Numbers

California and many other states restrict the use and disclosure of Social Security numbers.<sup>7</sup> For example, companies are not permitted to require individuals to transmit their SSNs over unsecured or unencrypted Internet connections. Similarly, SSNs cannot be printed on access or

identification cards, publicly posted or included on most documents mailed to the individual.

### Online Privacy Notices

Since July 2004, commercial website operators that collect information from California residents have been required to conspicuously post a privacy policy statement on their websites.<sup>8</sup> To comply, each privacy notice must:

- (1) Identify the categories of personal information that the website operator collects as well as the categories of third parties with whom it may share that information;
- (2) Provide a description of any process that exists for consumers to access or correct their information;
- (3) Describe the process by which the operator notifies consumers of material changes to the privacy policy; and
- (4) Identify its effective date.

The law also includes specific requirements for the privacy notice posting, to ensure that it is conspicuous.

### Conclusions

Most companies try to build compliance controls using a single national compliance standard, but it important not to lose sight of these California nuances. Because these laws contain private rights of action and statutory damages, they must be respected when doing business in the Golden State.

<sup>1</sup> CA Civil Code §1798.82

<sup>2</sup> CA Civil Code § 1798.81.5

<sup>3</sup> CA Civil Code § 1798.83-.84

<sup>4</sup> Financial institutions, small business and some other companies are exempt.

<sup>5</sup> CA Civil Code § 1747-1748.7

<sup>6</sup> 133 Cal. Rptr.2d 465 (Cal. App. 2003)

<sup>7</sup> See CA Civil Code § 1798.85

<sup>8</sup> CA Bus and Prof Code § 22575-22579

## Privacy Studio Speaks Out Security Breaches

If you want to learn more about data security requirements, network with your colleagues or just get some needed CLE or CPE credit, join Peggy at the ACI's 3rd Annual Legal & Operational Forum on **Preventing and Responding to Security Breaches** on September 28-28 in New York City.



More information about this excellent conference can be found online at [http://www.americanconference.com/Regulatory\\_Combpliance/breaches.htm](http://www.americanconference.com/Regulatory_Combpliance/breaches.htm)

As a speaker, Peggy can offer her clients and friends a **\$200 discount** — just mention promotional code **606L07.S**

This newsletter is intended for clients and friends of Privacy & Information Management Services—Margaret P. Eisenhauer, P.C. PIMS is a Georgia Law Firm specializing in privacy, security and information management. If you do not wish to receive communications from PIMS, please email [tanya@privacystudio.com](mailto:tanya@privacystudio.com)—we will gladly remove you from our mailing list.

The information contained in this newsletter has been prepared for informational purposes only and is not legal advice. This communication is not intended to create an attorney-client relationship. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials. If you are not a current client of PIMS, please do not send any confidential information.

Privacy & Information Management Services—Margaret P. Eisenhauer, P.C.  
4355 Cobb Parkway—Suite J-280, Atlanta GA 30339  
Phone: 404-914-1163  
[www.privacystudio.com](http://www.privacystudio.com)