COVINGTON

New State Privacy Laws Go Into Effect on Jan. 1, 2015

December 22, 2014

Privacy & Data Security

State legislators have recently passed a number of bills that impose new data security and privacy requirements on companies nationwide. The laws include new data breach notification requirements, marketing restrictions, and data destruction rules. Below is an overview of the new laws and amendments that will go into effect on January 1, 2015.

Amendments to California's Data Security and Breach Notification Law

In October 2014, California Governor Jerry Brown signed into law California bill AB 1710, an amendment to California's existing data security and breach notification law. As a result, the following changes to California's law will go into effect on Jan. 1:

1. *Companies that maintain personal information about Californians will need to implement and maintain reasonable security procedures and practices.*

California's current data security and breach law requires companies that own or license personal information about Californians to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information." For purposes of this data security requirement, California defines "personal information" as an individual's first name (or first initial) and her last name in combination with her social security number, driver's license or California ID number, any medical information, or a financial account number (such as a credit or debit card number) and the associated access code.

Under existing law, the terms "own" and "license" include personal information retained as a part of a business's internal customer accounts or for the purpose of using the information in transactions.

As of Jan. 1, California law will require companies that merely "maintain" personal information about Californians (such as cloud providers), but do not own or license the information, also implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

2. *Companies that maintain personal information about Californians will be required to immediately notify the owner or licensee of the personal information in the event of a breach.*

California currently requires companies that own or license personal information to disclose a data breach where it is reasonably believed that unencrypted personal information about a Californian was acquired without authorization. Current law also provides that such disclosure be made "in the most expedient time possible and without unreasonable delay."

As of Jan. 1, companies that maintain personal information will be required to notify the owner or licensee of the personal information "immediately" after discovery of a breach if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

For purposes of data breach disclosure, "personal information" includes login credentials ("[a] user name or email address, in combination with a password or security question and answer that would permit access to an online account,") as well as an individual's first name (or first initial) and her last name in combination with her social security number, driver's license or California ID number, any medical information, or a financial account number (such as a credit or debit card number) and the associated access code.

As a reminder, other than for user name and password breaches (discussed below), current California law requires that a breach notification must be written in plain language and must include specific types of information about the breach.

Where the security breach involves the breach of online account information and no other personal information, then California law requires a business to provide the security breach notification in electronic or other form, directing the person whose personal information has been breached to promptly change her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with that business as well as all other online accounts for which the person uses the same name or email address and password or security question or answer.

However, where the security breach involves the breach of login credentials of an *email account* provided by a business, the business must not send the security breach notification to that email address. Instead, the business may comply with California law by providing notice by hard copy written notice or by clear and conspicuous notice delivered to the individual online when the individual is connected to the online account from an IP address or online location from which the business knows the resident customarily accesses the account.

3. *After a breach, companies **might** be required to provide free identity theft prevention and mitigation services for 12 months.*

AB 1710's co-author stated in a press release that the bill "[r]equires the source of the breach to offer identity theft prevention and mitigation services for 12 months at no cost to individuals affected by a data breach. However, it is not clear whether this position is supported by the text of the bill, which only states that "if any" identity theft prevention and mitigation services are to be provided, then such services must be provided for 12 months at no cost. An earlier version of the bill had stated that identity theft and mitigation services "*shall be* provided" to individuals affected by a data breach.

Given the ambiguity of the requirement to provide free identity theft prevention and mitigation services, whether and how this provision will be enforced in 2015 is something to watch.

4. *Companies may not sell, advertise for sale, or offer to sell an individual's social security number.*

The amendment also includes a new prohibition on social security numbers. As of Jan. 1, California law will prohibit the sale, the advertisement for sale, and the offer to sell an

individual's social security number. Businesses that own, license, or maintain information on an individual's social security number will want to keep this new prohibition in mind when contemplating data transfer or broker agreements, or other transactions involving the personal information of Californians.

California's New Minor Privacy Marketing and Privacy Law

California's "Privacy Rights for California Minors in the Digital World Law", SB 568, (1) bars some online operators from marketing certain products and services to minors, and (2) allows minors under 18 to request deletion of certain content from websites on which they have registered (known informally as the "eraser law.")

1. *Restrictions on Marketing to Minors*

Operators of websites, online services, online applications, and mobile applications that are directed to minors are prohibited from marketing or advertising the following products and services:

- Alcoholic beverages
- Tobacco, cigarette, or cigarette papers, or blunt wraps, or any other preparation of tobacco, or any other instrument or paraphernalia that is designed for the smoking or ingestion of tobacco, products prepared from tobacco, or any controlled substance
- Electronic cigarettes
- Salvia divinorum or Salvinorin A, or any substance or material containing Salvia divinorum or Salvinorin A
- Drug paraphernalia
- Firearms or handguns, ammunition or reloaded ammunition, handgun safety certificates, BB device
- Less lethal weapons
- Dangerous fireworks
- Aerosol containers of paint capable of defacing property
- Etching cream capable of defacing property
- Tanning in an ultraviolet tanning device
- Dietary supplement products containing ephedrine group alkaloids
- Tickets or shares in a lottery game
- Body branding or permanent tattoos
- Obscene matter

These operators also are prohibited from: (1) knowingly using, disclosing, or compiling a minor's personal information for the purposes of marketing or advertising any of those prohibited products or services, and (2) knowingly allowing a third party to use, disclose, or compile the minor's personal information to market or advertise these products or services.

If an operator has actual knowledge that a minor is using the services, the operator may not target marketing or advertising to that minor based on the minor's personal information. The operator also may not use, disclose, or compile the minor's personal information to market or advertise the prohibited products or services, nor may the operator allow a third party to use, disclose, or compile the minor's personal information for the prohibited products and services.

2. *Deletion Requirement*

If a minor is a *registered* user of a website, online service, online application, or mobile application, the operator must allow the minor to remove content and information that the minor had publicly posted on the website, service, or app. Operators also are required to provide notice of this right to registered minors.

Operators are not required to delete content or information if:

- Any federal or state law requires the operator to maintain the content or information;
- The content or information was provided by an individual other than the minor;
- The content or information is anonymized;
- The minor did not properly follow the instructions for requesting deletion; or
- The minor received compensation or consideration for providing the content.

Amendments to California's Invasion of Privacy Law

California's Invasion of Privacy law will also receive an update on January 1, 2015. The California Invasion of Privacy law currently prohibits the attempt to capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression, when the person is engaged in a personal or familial activity under circumstances where they had a reasonable expectation of privacy. Current California law prohibits the activities described where the attempt to capture is done through a visual or auditory enhancing device. As of January 1, 2015, the above activities will be prohibited when done using *any* device.

Amendments to California's Revenge Porn Law

California's current Revenge Porn law prohibits the posting online of nude or sexually explicit pictures of an individual without their consent where the poster knew that the other person had a reasonable expectation that the material would remain private. The current law provides for a jail term of up to six months. The amendment to California's Revenge Porn law creates a private right of action against individuals who engage in the activities described above.

New Delaware Data Destruction Law

Companies conducting business in Delaware will be required to take all reasonable steps to destroy or arrange for the destruction of a consumer's personal identifying information when those records are no longer retained. Destruction may occur by shredding, erasing, or otherwise destroying or modifying the personal identifying information so as to render the information unreadable or indecipherable.

The Delaware law defines personal identifying information as a consumer's first name or first initial and last name in combination with one of the following: signature; date of birth; social security number; passport number; driver's license or state identification card number; insurance policy number; financial services account number, bank account number, credit card number, or other financial information; or confidential health care information.

Entities subject to the Gramm-Leach-Bliley Act, covered entities subject to HIPAA, and consumer reporting agencies subject to the FCRA are exempt from the new law. Other entities,

however, may be subject to private enforcement actions, which allow for the recovery of treble damages. These have the potential to add up quickly, as each record unreasonably disposed of constitutes a violation under the statute. In addition, the Delaware Attorney General and Division of Consumer Protection of the Department of Justice may bring suit in certain circumstances.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Privacy & Data Security practice group:

David Fagan	+1 202 662 5291	dfagan@cov.com
Kurt Wimmer	+1 202 662 5278	kwimmer@cov.com
Jeff Kosseff	+1 202 662 5489	jkosseff@cov.com
Katie Gasztonyi	+1 202 662 5916	kgasztonyi@cov.com