# Privacy Alert: California Passes Trio of New Online Privacy and Data Security Measures

TYLER NEWBY, MICHAEL EGGER, STEFANO QUINTINI AND MADELINE ZAMOYSKI

Fenwick
FENWICK & WEST LLP

In the last month, the California legislature passed and Governor Jerry Brown signed into law amendments to two of California's signature privacy and data security laws and one new consumer privacy law aimed at enhancing privacy protections for minors. Although the trio of new laws are measured in their scope, as discussed below, they will require operators of websites and online services to make changes to their privacy policies as early as January 1, 2014, and may have the effect of significantly expanding companies' disclosure obligations following a data breach.

**AB 370 –Do Not Track Amendment to CalOPPA**

The passage of AB 370 marks the first law addressing Do Not Track ("DNT") signals sent from web browsers, even if it does not require advertisers or website operators to honor those signals. Instead, the law requires that operators of websites and online services, including mobile applications, notify users about how they handle DNT signals.

AB 370 does not create a standalone law, but amends the California Online Privacy Protection Act (CalOPPA), Cal. Bus. And Prof. Code Sections 22575-22579, and must be interpreted within that statute's requirements. CalOPPA requires operators of a website or online service to post a privacy policy if they collect "personally identifiable information" from consumers in California. CalOPPA defines personally identifiable information as "individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following:" (1) first and last name; (2) home or other physical address, including street name and name of a city or town; (3) email address; (4) telephone number; (5) social security number; (6) any other identifier that permits the physical or online contacting of a specific individual; or (7) information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision.

CalOPPA requires operators to make specific disclosures in their privacy policies regarding their collection and sharing of personally identifiable information. Effective January 1, 2014, AB 370 will also require operators to disclose in their privacy policies:

- how the operator responds to "do not track" signals sent by a consumer's browser or other mechanism that provides consumers a choice regarding the collection of personally identifiable information about an individual consumer's online activities over time and across third party websites and online service; and
- whether other parties (e.g., advertisers) may collect personally identifiable information about a consumer's online activities when that consumer visits the operator's website or online service.

AB 370 focuses on transparency, but is also limited to the collection of "personally identifiable information" as defined by CalOPPA. Due to this limitation, it is not clear whether the new disclosure obligations would apply to an operator or an authorized third party that collects log data, browser activity, or web protocol logs (through mechanisms that would otherwise respond to "do not track" signals) separately from and not in connection with any personally identifiable information.

Affected businesses will need to update their privacy policies by January 1, 2014, when the new law goes into effect. Businesses should consider starting discussions about company privacy practices, policies and how those will be communicated to users of its websites, online services and mobile applications well in advance of the effective date, as these discussions may take some time.

**SB 46 – Amendment to California's Data Breach Notification Law**

In 2002, California became the first state to enact a data breach notification law, requiring California businesses or businesses that own or license computerized data that includes personal information of California residents to disclose a breach of the security of that data. Since then, California has incrementally increased the scope of personal data subject to the notification law in the event of a breach as what must be disclosed in the notification. Effective January 1, 2014, California's will become the first state to require California businesses or businesses possessing data of California residents to disclose a breach of users' online account information.

Specifically, California Civil Code 1798.82 will be amended to require disclosure of the breach of "[a] user name or email address, in combination with a password or security question and answer that would permit access to an online account." This would likely include a breach of an email account username and password or username and password of a social networking service or online game. Increasingly, businesses have chosen to disclose such breaches voluntarily; Cal. Civil Code § 1798.82 will make those disclosures mandatory, and hold companies to the law's requirements on the content of the notice and how notice is to be delivered.

The amendment creates specific notification options and requirements for breaches of online account information. The business may give electronic notice to the affected account holders by "promptly" directing them to change their passwords, security questions or answers or to take "other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer." This notice method applies only where the only information that has been breached is a user's online account information. If other information, such as a user's first and last name plus a social security number is breached, the business must comply with the notice provisions set forth in Section 1798.82(j). However, if the breached account is an email account, the business may not give notice to affected users by email. Instead, they may give notice by any other means specified by Section 1798.82(j) or by "clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account."

Because many businesses that are affected by data breaches do not possess the types of personal information that have been subject to statutory breach notifications, many data breaches have gone unreported. Amendment 1798.82 will likely have the effect of increasing the number of data breaches reported, at least in the near term.

**SB 568 – "Privacy Rights for California Minors in the Digital World" – The Minor "Eraser" Law**

On January 1, 2015, California's new law entitled "Privacy Rights for California Minors in the Digital World" will go into effect as Cal. Bus. & Prof Code Sections 22580-22582.

Enacted to address the privacy of minors (defined as California residents under the age of 18), the law requires website and mobile app operators to provide minors with (i) the ability to remove or request removal of content that the minor posted on the website or mobile app; (ii) notice and clear instruction on how to do so; and (iii) notice that such removal may not remove all traces of such posting. For the removal requirement, operators can comply by making the original content invisible to other users and/or the public, even if it remains on the operator's servers or if a third party has copied the content and made it available elsewhere. Operators may not have to comply with the removal requirement if: (i) federal or state law requires maintenance of the content or information; (ii) the content was stored or posted (or reposted) by a third party other than the minor; (iii) the operator anonymizes the content or information so that the minor cannot be identified; (iv) the minor received compensation or other consideration for providing the content; or (v) the minor does not follow

the instructions provided by operator to request removal of content.

The law also places restrictions on advertising to minors. It prohibits operators of websites and mobile apps from (i) marketing or advertising certain products to minors if the marketing or advertising is directed to that minor based upon information specific to that minor, e.g., profile, activity, address, location sufficient to establish contact; and (ii) using, disclosing or compiling personal information of a minor (or allowing third parties to do so) with the actual knowledge that it will be used for marketing or advertising certain restricted products. The restricted products include alcoholic beverages, handguns, ammunition, spray paint, tobacco products, fireworks, tanning services, dietary supplements, lottery tickets, tattoos, drug paraphernalia, obscene matter, and other products and services. Operators can comply by (i) taking "reasonable actions in good faith" to avoid such marketing or advertising; or (ii) notifying the adverting service that the website or mobile app is "directed to minors," at which point the obligation to refrain from marketing to minors shifts to the advertising service.

An operator must comply with the removal requirements if its website or mobile app is "directed to minors" (as opposed to general audiences) or if the operator has actual knowledge that a user is a minor. Operators are not required to collect or maintain age information under the new law, so operators that do not collect this information and operate general audience websites or mobile applications may not be affected. It is not clear whether a portion of a general audience website that becomes "directed to minors" would require an operator's compliance with the new law. While the law contemplates several circumstances in which an operator would not be required to comply with the removal requirements, this circumstance is not among them.

For more information please contact:
Tyler Newby, 415.875.2495,
tnewby@fenwick.com

Michael Egger, 415.875.2326,
megger@fenwick.com

Stefano Quintini, 650.335.7696,
squintini@fenwick.com

Madeline A. Zamoyski, 650.335.7639,
mzamoyski@fenwick.com