Skadden

PRIVACY & CYBERSECURITY UPDATE

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP & AFFILIATES

October 2013

Recent Changes to California Privacy Law Have Nationwide Implications

Several key developments have taken place in the privacy arena in the last few weeks. California expanded both its privacy policy and data breach notification laws in ways that will have national implications. The FTC made its first foray into regulating the "Internet of Things" by bringing an enforcement against a home security camera manufacturer. And, the Fifth Circuit gave new life to plaintiffs in data breach cases by finding that the economic loss doctrine did not bar data breach negligence claims in certain situations. We address each of these developments below.

California Expands the Scope of Its Data Breach Notification Law

In 2003, California created an entirely new body of law when it became the first state to adopt a data breach notification requirement. Since then, almost every state has followed California's lead and enacted identical or similar requirements. This month, California has taken the lead in this area once again, expanding the types of personal information that would trigger the notice requirement if their security is breached.[1]

Currently, notification must be sent to any resident of California 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 and last name in combination with any one or more of the following data elements, when either the name or the data elements are unencrypted:

(1) Social Security number.

(2) Driver's license number or California identification card number.

(3) Account number or 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.

(4) Medical information.

(5) Health insurance information.

The new amendment expands personal information to include a user name or email address, in combination with a password or a security question and answer that would permit access to an online account.[2] Therefore, even if a business does not hold any of the data elements that could trigger notice under the old law (*e.g.*, a Social Security number), notice of a breach would be required if a user name and password or security question and answer were compromised.

Once a notification obligation is triggered, obligations surrounding the delivery of the notification itself remain largely unchanged from the current law. However, for breaches that involve *only* login and password information of nonfinancial accounts, companies may satisfy the notification

1 Sections 1798.29 and 1798.82 have similar effect with Section 1798.29 applying to state agencies and Section 1798.82 applying to persons or businesses that conduct business in California. The full text of these laws, as amended, can be found at: www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0001-0050/sb_46_bill_20130906_enrolled.htm.

2 Prior to the enactment of this amendment, a user name/password combination was subject to data breach notification only if such information could permit access to a financial account. See Sections 1798.29(g)(3) and 1798.82(h)(3) of the California Civil Code.

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact **Stuart D. Levi** at 212.735.2750 or stuart.levi@skadden.com, or your regular Skadden contact.

* * *

Four Times Square
New York, NY 10036
Telephone: 212.735.3000

WWW.SKADDEN.COM

obligations by providing the affected individuals with electronic notice prompting them to reset their passwords. If the breach involves the login and password information of an email account that the business makes available to the individual (*e.g.*, an email address @ the breaching party's domain), the notification must be made by means other than an email sent to the breached email account.

While the law only applies to California residents whose data has been breached, the amended law may effectively set the nationwide notification standard for many companies. Specifically, companies that face data breaches involving user names and passwords may not want to provide notice only to impacted California residents. Rather, in order not to treat their customers differently, companies hit by such a data breach may simply opt to provide notice to all impacted users.

California Adds a "Do Not Track" Disclosure Requirement for Online Privacy Policies

To date, California has been the only state to require that certain websites post a privacy policy. Specifically, under the California Online Privacy Protection Act (Sections 22575-22579 of the Business and Professions Code) operators of commercial websites or online services that collect personally identifiable information (PII) about California consumers must conspicuously display a privacy policy that: (i) identifies the PII collected and explains how it is shared, (ii) contains directions for reviewing or correcting PII (if the user is so permitted), (iii) explains how the user will be notified of changes to the policy, and (iv) identifies the effective date. On September 27, California enacted an amendment to that law (A.B. 370) that requires two additional and significant disclosures in such privacy policies:

- ***Disclose how the operator responds to browser "do not track" signals***. If the operator of a website engages in the collection of PII about an individual consumer's online activities over time and across third-party websites or online services, the privacy policy must disclose how the operator responds to Web browser "do not track" signals or other mechanisms that provide consumers with the ability to exercise choice regarding the collection of such PII. This requirement may be complied with by providing a conspicuous hyperlink within the privacy policy to a description of any program or protocol the operator follows that offers such choice. "Do not track" signals are settings offered on browsers that allow consumers to block their activities from being tracked by third-party advertisers and other sites they have not visited.

  The new California requirement comes at a time when (DNT) practices are being fiercely debated by technology companies and online advertisers. The central issue is whether, and how, advertisers will honor DNT settings and whether these settings should be pre-set to the "do not track" option (as opposed to requiring consumers to activate the blocking). Attempts by the World Wide Web Consortium to develop and implement an industry-wide standard so far have failed.

- ***Disclose whether third parties may collect PII from the website's users***. If the operator of a website allows third parties to collect PII about a user's online activities over time and across different websites, the operator must disclose that fact within the privacy policy. This effectively requires websites to disclose if they allow third-party advertisers to track the user's online activities.

The amendment is effective immediately, although operators who receive a notice of noncompliance with the above privacy policy requirements have 30 days to bring their policy into compliance. A failure to do so may result in statutory penalties of up to $2,500 for each violation under California's Unfair Competition Law. These requirements are the first of their kind to be codified into law within the United States, though they are within the scope of the FTC's Self Regulating Principles for Online Behavioral Advertising proposed in 2009, and, therefore, privacy policies written to adhere to these Self Regulating Principles should already be in compliance.

The FTC Brings Its First Enforcement Action Against the 'Internet of Things'

Although the "Internet of Things" might sound like something cooked up by the Monty Python comedy troupe, it is a serious concept and represents the newest frontier in the FTC's efforts to protect consumer privacy. The Internet of Things is the term given to the network of physical products that can be remotely and uniquely identified because of embedded sensors or other devices. Pacemakers, roads, items in inventory and farm equipment are all examples of physical products that can transmit dynamic data about their location, performance and other attributes. As physical products become interconnected in an Internet-like fashion, the potential for business use, and hacker abuse, will grow exponentially.

The FTC has become increasingly focused on the issues raised by this technology and has scheduled a public workshop on the Internet of Things" for this November. Last week, in further proof of its interest in this area, the FTC brought its first enforcement action against a provider of Internet-connected hardware. The defendant, TRENDnet, is a provider of Internet protocol home security video cameras that allow consumers to monitor their homes remotely. TRENDnet's camera system was hacked and live footage from cameras installed in people's homes was posted on the Internet. The FTC alleged in its complaint that the marketer had, among other things, failed to use reasonable security to design and test its software, and had transmitted login credentials "in clear, readable text over the Internet, even though free software was available to secure such transmissions."

The FTC settled with TRENDnet and its consent decree the FTC prohibits TRENDnet from misleading consumers about the security of its device, and requires the company to design and implement a written comprehensive security program with technical, administrative and physical safeguards. TRENDnet also is required to notify all of its customers regarding the breach.

The TRENDnet action highlights the FTC's interest in the Internet of Things and its continuing enforcement activity against companies that the FTC believes are not implementing appropriate privacy safeguards to protect consumers.

Fifth Circuit Ruling Provides New Avenue of Attack for Data Breach Plaintiffs

Plaintiffs in data breach cases often find that their claims are dismissed because of the "economic loss doctrine," *i.e.*, that a plaintiff cannot recover under a negligence claim if its losses are economic. Since most data breach claims are based on the negligence of the entity holding the plaintiff's data, and since their losses are inevitably economic, this doctrine presented a seemingly insurmountable bar. However, a recent decision by the Fifth Circuit in *Lone Star Nat'l Bank N.A. v. Heartland Payment Sys., Inc.*, suggests that at least in some states such a bar does not exist.

The *Heartland* case involves one of the most well-known data breaches. In 2008, hackers infiltrated the data systems of Heartland, a credit card processing company, resulting in a data breach that exposed over 130 million customer records — including credit and debit card data — and caused billions of dollars in damages, including losses suffered by the banks that issued the credit and debit cards. These issuing banks bore the expense of replacing the cards and also refunding customers for fraudulent charges that were made on the stolen cards before they could be deactivated.

The issuing banks did not have a contractual relationship with Heartland; rather, all contracts were between Heartland and the banks used by the merchants (the "acquiring banks"). In effect, the acquiring banks would contract with Heartland, which would serve as the processor between the acquiring banks and the issuing banks, all of whom were operating under the VISA and Mastercard regulations.

When the issuing banks sued Heartland for the negligence that led to the breach, the trial court dismissed the action, finding that Heartland was protected by the economic loss doctrine, since the issuing banks could only assert economic losses. The Fifth Circuit reversed, finding that under

New Jersey law (although not Texas law) the economic loss doctrine did not create such a bar. The Fifth Circuit held that although New Jersey law follows the economic loss doctrine, it creates an exception where there is an identifiable class of plaintiffs "whom the defendant knows or has reason to know are likely to suffer such damages from its conduct." In deciding whether the harm to such a group was foreseeable, the court looked to "the certainty or predictability of their presence, the approximate numbers of those in the class, as well as the type of economic expectations disrupted." The court also noted that under New Jersey law, tort recovery was available for economic losses "only when the plaintiff lacks another remedy."

In the case before it, the Fifth Circuit found that the issuer banks were clearly an identifiable class, since Heartland could have foreseen that its negligence in failing to prevent a data breach would cause the issuer banks to suffer economic losses, and it knew the identity of these entities, since they were "the very entities to which Heartland sends payment card information." The court also concluded that without such a tort remedy, the issuer banks would seem to have no remedy, which would defy notions of "fairness, common sense and morality."

Although the Fifth Circuit's opinion is limited to New Jersey law, given the national scope of many data breaches, the Fifth Circuit has opened the door for plaintiffs to argue in New Jersey that they may sustain a negligence claim for data breaches even if their only loss is economic in nature. The decision therefore could significantly expand a company's financial exposure in the event of a cyber-attack.