March 2024

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

Maine Bill Requires ISPs to Obtain Opt-In Consent from Customers

The Maine legislature has passed a bill that requires internet service providers (ISPs) operating in Maine to obtain express, affirmative consent from customers before using, disclosing, selling or permitting access to a customer's personal information, which would include web-browsing history, application-usage history, geolocation information, financial information and health information. With certain exceptions, the bill would prohibit a provider from "refusing to serve a customer, charging a customer a penalty or offering a customer a discount if the customer does or does not consent to the use, disclosure, sale or access." If signed by Governor Janet Mills, the law would take effect July 1, 2020.

TAKEAWAY

Prescriptive requirements requiring opt-in consent are onerous and even more stringent than the opt-out requirements of the California Consumer Privacy Act (CCPA). Companies need to pay close attention to updates like this to properly implement policies and procedures to remain in compliance with state and federal laws.

Nevada Law Allows Consumers to Opt Out of Companies Selling Their Data

Taking a piecemeal approach to updating Nevada's privacy laws, Governor Steve Sisolak has approved amendments to Chapter 603A (Privacy and Security of Personal Information). The revised law, which will become effective October 1, 2019, will provide consumers the right to opt out of the sale of their personal information. This new right, though similar on its face, is

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Al Saikali
Chair, Privacy and Data Security Practice
305.358.5171
asaikali@shb.com

narrower than the right provided by the CCPA; the Nevada law will apply only to online activities and has a much more restrictive definition of "sale." Nevertheless, the law will impose compliance costs on businesses that offer websites or online services by requiring them to provide means for consumers to submit verified opt-out requests and to honor those requests.

TAKEAWAY
Allowing consumers to stop the sale of their information is a growing trend that brings a wave of compliance and operational headaches.

Health Insurer Reaches $74 Million Class-Action Settlement

Seattle-based Premera Blue Cross reportedly reached a settlement agreement for $74 million to resolve a combined class action that was based on a data breach affecting 10.6 million plan members. Some $32 million of that amount will go directly to victims of the breach. Another portion of the settlement will give victims two extra years of credit monitoring and other identity-protection services, while the company will use the remaining funds to implement a robust information-security program during the next three years. The company has already taken steps to strengthen its security by achieving HITRUST certification, which "demonstrates the ability of the company to identify risks, protect data, detect cyberattacks, and respond to data breaches."

TAKEAWAY
Fortify your information-security program before a breach occurs.

Texas Updates Breach-Notification Requirements

After numerous amendments, the Texas legislature passed House Bill 4390, which strengthens the state's breach-notification law. If signed by the governor, the law will require companies suffering a breach of security to disclose certain information to the attorney general's office for breaches affecting at least 250 Texas residents. The law would also impose a deadline to provide notification 60 days "after the date on which the person determines that the breach occurred."

In addition to the breach-notification changes, the bill also creates the Texas Privacy Protection Advisory Council to study and evaluate privacy laws in Texas and to recommend changes to the Texas legislature by September 1, 2020.

Colman McCarthy
Associate
816.559.2081
cdmccarthy@shb.com

Kate Paine
Associate
813.202.7151
kpaine@shb.com

Ben Patton
Associate
206.344.7625
bpatton@shb.com

TAKEAWAY

States are hesitant to adopt comprehensive consumer-privacy bills similar to the CCPA but are still updating their breach-notification laws with more strict requirements.

Standing Found in Missouri Privacy Case Based on State Statute

A Missouri hospital may be on the hook for damages under the Missouri Merchandising Practices Act (MMPA) stemming from an employee posting a child's medical data and personally identifiable information on an unauthorized website. The court determined the plaintiff had standing for her MMPA claim based on an overpayment theory. The statute provides a private right of action if a person "sustains ascertainable loss" as a result of unlawful acts, and the plaintiff alleged she overpaid for services due to the inadequate protection of her information. Separately, the court found standing for (though it ultimately dismissed) the plaintiff's breach-of-contract claim directed to the hospital's privacy policy based on a theory that she had been denied the benefit of the bargain for that policy.

TAKEAWAY

Courts may find standing in privacy litigation outside of the context of direct monetary harm like identify theft.

NJ Amends Data-Breach-Notification Law

New Jersey has enacted an amendment to its data-breach-notification law requiring the disclosure of security breaches affecting online accounts. The amendment modifies the definition of personal information to include "user name, email address, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account." The law also provides other prescriptions regarding the form of notice and will take effect September 1, 2019.

TAKEAWAY

Look for more states to include online-account information as part of their data breach notification laws. Encrypting online-account information, including security questions and answers, will help reduce exposure.

Medical IT Company Settles Potential HIPAA Violations

HIPAA regulations require companies to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information." An Indiana software and EMR-services provider has agreed to pay $100,000 to the Office for Civil Rights after it failed to conduct that type of comprehensive risk analysis prior to a 2015 breach affecting approximately 3.5 million individuals. As part of the resolution, the company agreed to complete a company-wide risk analysis within 30 days and annually thereafter.

TAKEAWAY

This underlines the importance of performing a risk assessment before a company suffers a data incident.

Illinois Breach-Notification Update Goes to the Governor

Illinois lawmakers have passed Senate Bill 1624, which now awaits Governor J.B. Pritzker's signature. The bill, which amends the Illinois Personal Information Protection Act, requires entities to notify the state attorney general's office about security breaches affecting more than 500 Illinois residents. Following other state breach-notification laws, the Attorney General's office now must be notified "in the most expedient time possible and without unreasonable delay but in no event later than when notice is provided to the consumer." Additionally, the bill grants the attorney general authority to publish information concerning security breaches such as the name of the data collector who suffered the breach and the types of personal information compromised in the breach.

TAKEAWAY

Companies should verify all state breach-notification requirements in the case of a data breach, including when to notify state regulators.

Singapore and Hong Kong Agree to Share Data Breach Information

Regulators in Hong Kong and Singapore have reportedly signed a memorandum agreeing to share data-breach information, research and other experiences related to data protection. Hong Kong's privacy commissioner and Singapore's deputy commissioner of personal-data protection reached the resolution after discussions began in September 2018 following several major data breaches in both jurisdictions.

TAKEAWAY

Collaboration across companies and jurisdictions strengthens data protection.

FCC Looks to Indirectly Crack Down on Robocalls

Consumers may see additional relief from unwanted robocalls after the Federal Communications Commission (FCC) approved a proposal allowing wireless carriers to "aggressively block" robocalls for customers, which would include allowing default blocking based on "reasonable call analytics." Consumers will still be able to block unknown numbers themselves and have the option to opt in or out of any blocking services offered by their carrier. However, some companies are reportedly concerned that the use of "reasonable call analytics" may unintentionally block calls from legitimate sources that use auto-dialing features such as doctors' offices, pharmacies and credit card fraud-detection programs.

TAKEAWAY

Long-awaited FCC action could provide relief to consumers, but it could also result in blocking of legitimate calls.