Having trouble reading this email? View it in your browser.

March 2024

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

The Legal 500 Adds Shook to Top Rankings in Cyber Law

The Legal 500 United States has again recognized Shook, Hardy & Bacon as one of the premier litigation firms in the country, giving top marks to a variety of practices, including the firm's Privacy and Data Security Practice. The organization recognized Shook's areas of strength in "biometric privacy, incident preparation and response, GDPR compliance, vendor management, international data transfer as well as litigation and dispute resolution."

Shook's Privacy and Data Security Practice includes Al Saikali (Practice Chair), Melissa Siebert (Director of the firm's Biometric Privacy Task Force), Tristan Duncan, Gary Miller, Bill Sampson, Matthew Wolfe, Erin Hines, Colman McCarthy, Kate Paine, Benjamin Patton, Lischen Reeves, Palak Shah, Erika Dirk, Ian Hansen, Benjamin Sedrish, and Jonathon Studer.

States Continue to Lead the Way on Privacy Legislation

TAKEAWAY

Unless and until preemptive federal legislation is passed, the patchwork of state privacy laws will continue to expand and diversify.

New York Privacy Act Would Create Private Right of Action

Introduced on May 9, 2019, the New York Privacy Act continues the trend of states considering broader, privacy-focused

SUBSCRIBE

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

legislation. The Act would require companies to disclose their methods of de-identifying personal information, place special safeguards around data sharing, and allow consumers to obtain the names of all entities with whom their information is shared. Also included is a private right of action for any violation of the Act, though no provision is made for statutory damages; plaintiffs would be limited to actual damages and attorney's fees. The bill is currently awaiting action by the Senate Consumer Protection Committee.

Update: Maine Bill Signed into Law Requiring ISPs to Obtain Opt-In Consent from Customers

Following Governor Janet Mills' signature, Maine's privacy law will take effect on July 1, 2020. The law requires 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 discriminating against customers who refuse to provide consent.

Oregon Enacts Amendments to Data Breach Notification Law

Oregon Governor Kate Brown has approved five amendments to the Oregon Consumer Identity Theft Protection Act (including a name change to the "Oregon Consumer Information Privacy Act"), with the changes taking effect January 1, 2020. The amendments impose additional reporting requirements in the event of a breach (such as notification to the attorney general when more than 250 consumers are affected), redefine the term "covered entity," expand the definition of personal information to include online-account information, and allow vendors and covered entities to use their compliance with federal data-security laws as an affirmative defense to violations of the Act.

Bill to Exempt Employee Information from CCPA Advances and Changes

AB 25, one of the most closely watched bills that would amend the California Consumer Privacy Act (CCPA), overcame a major hurdle by passing the California Assembly shortly before the May deadline to do so. A June 28 amendment then made significant changes to the structure and content of the bill. Previously, AB 25 modified the definition of "consumer" to exclude employees, etc., but the later amendment cancels that definition change in favor of three explicit exemptions from the CCPA for the personal information of "a job applicant to, an employee of, owner of,

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

Lischen Reeves
Associate
816.559.2056
lreeves@shb.com

director of, officer of, medical staff member of, or contractor of" a business where the information is collected and used: 1) solely within the context of that person's role; 2) as emergency-contact information; and 3) to administer benefits. (Definitions are also provided for the various individuals covered by the exemptions.)

The amendment to AB 25 would also allow businesses to require reasonable authentication of a consumer and to require a consumer to submit a request through her account if she maintains one with the business.

Shook Achieves Seventh Circuit Victory in BIPA Suit for Improper Venue

In *Miller v. Southwest Airlines,* the Seventh Circuit determined that the plaintiffs—unionized employees of Southwest Airlines—must pursue their claims under the Illinois Biometric Information Privacy Act (BIPA) using the Railway Labor Act's union-grievance procedures rather than through a class action in court. Due to the collective-bargaining agreements between Southwest (represented by Shook's Melissa Siebert) and the employee union, the court found that "there can be no doubt that how workers clock in and out is a proper subject of negotiation between unions and employees" and is a mandatory subject of bargaining between the parties.

TAKEAWAY
Despite the *Rosenbach* decision lowering the bar for BIPA claims to get into court, other avenues are available for defendants to challenge the propriety of BIPA actions.

Controversial "Hack Back Bill" Reintroduced

Undeterred by vehement pushback to the original bill introduced in 2017, a bipartisan group of lawmakers has reintroduced the Active Cyber Defense Certainty Act (affectionately known as the "Hack Back Bill"). The bill aims to arm companies with the ability to use active-defense techniques that could otherwise give rise to liability under the Computer Fraud and Abuse Act (though the bill would offer no immunity from civil suits). Hacked companies would be able to turn the tables and penetrate a hacker's system, but only to find out what happened to stolen information and to gather information for U.S. law enforcement. The bill would *not* allow a company to "impair essential functionality or install backdoors on the attacker's system." And—thankfully—the bill requires both FBI review of defense techniques and notice to the

FBI before the hacking is carried out. Numerous experts have raised concerns about the vague scope of the bill and the potential for harm to innocent individuals when hack backs go wrong.

TAKEAWAY

In the end, the Hack Back Bill is unlikely to become law, but its revival signals the onset of more high-profile efforts to enact privacy and security legislation.

The choice of a lawyer is an important decision and should not be based solely upon advertisements.

© Shook, Hardy & Bacon L.L.P. All rights reserved.

Unsubscribe | **Forward to a Colleague** | **Privacy Notice**