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

March 2024

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

Florida Introduces BIPA Legislation

A Florida state senator has introduced an identical version of the Illinois Biometric Information Privacy Act (BIPA). The private right of action could lead to a wave of biometric-privacy lawsuits filed in Florida similar to the surge that BIPA has caused in Illinois. However, the bill faces an uphill battle to becoming law because of the political makeup of the Florida state legislature. Regardless of whether the bill gains momentum, the Florida legislature must seriously consider the substantial effect this law will have on companies of all sizes.

Read the bill text >>

Federal Privacy Legislation Debate Continues

U.S. lawmakers are debating options and hearing from industry and interest groups about establishing a federal privacy law. Hot topics include whether the United States should adopt an adaptation of the EU model or whether new federal privacy rules should preempt stricter state laws such as the California Consumer Privacy Act of 2018. While a majority of lawmakers agree that greater transparency and tougher enforcement is needed to protect consumer data, they have not reached a consensus on what model the United States should adopt.

Read more at *Phys.org* >>

Record COPPA Fine Issued

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

The U.S. Federal Trade Commission (FTC) has issued its largest civil penalty ever under the Children's Online Privacy Protection Act (COPPA). Social networking app Musical.ly (now TikTok) agreed to pay $5.7 million for allegations that the app failed to notify parents or seek parental consent before collecting information from users under the age of 13. In addition to the monetary settlement, Musical.ly agreed to remove all videos made by children under 13.

Read the FTC press release >>

Aetna Reaches Settlement with California over Privacy Breach

Aetna has reached a $935,000 settlement with California regarding alleged violations of state health-privacy laws. The allegations stemmed from a 2017 incident in which Aetna sent letters to approximately 12,000 people across the United States revealing via a windowed envelope that the recipients were taking HIV medication. California Attorney General Xavier Becerra referred to the incident as a "gross privacy violation" of the 1,991 Californians who received the letters. Under the settlement terms, a designated employee at Aetna must implement and maintain specific procedures and other privacy policies to ensure that medical information is not revealed through envelope windows. Additionally, Aetna must complete an annual privacy risk assessment for three years.

Read the California attorney general's press release >>

Community Health Systems Settles Claims over Stolen Patient Data

Tennessee-based Community Health System (CHS) has agreed to settle claims arising out of a 2014 data breach that exposed personal health information for 4.5 million individuals. The incident, which occurred between April and June 2014, was the result of an advanced malware attack launched from China designed to obtain sensitive information. The settlement, which caps the amount for class claims at $3.1 million, is awaiting court approval. The plaintiffs alleged that CHS failed to implement and follow basic security procedures to safeguard the information.

Read more at *Bank Info Security* >>

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

Proposed Amendments to BIPA Introduced

Illinois Rep. Michael Madigan has introduced House Bill 669 to amend the state's Biometric Information Privacy Act (BIPA). While the amendment only includes a technical change to the short title of BIPA, additional language could be added when the bill is voted out of committee. Under-the-radar amendments to BIPA could have significant impacts if the legislature adds supplementary language.

Additionally, Illinois Sen. Jason Barickman introduced an amendment to BIPA that would rescind the private right of action currently provided by the statute, instead placing enforcement authority with the Department of Labor. The amendment also provides that a violation of BIPA constitutes a violation of the Illinois Consumer Fraud and Deceptive Business Practices Act and may be enforced by the state attorney general. The amendment states that it would be "effective immediately" upon passage but there is no indication regarding the applicability to already-filed suits.

Finally, Illinois House Bill 3024 proposes an amendment to BIPA related to the definition of a "biometric identifier." Specifically, the amendment proposes adding "electrocardiography result[s] from a wearable device" as a biometric identifier. However, the amendment does not specifically define what constitutes a "wearable device."

CNIL-Imposed GDPR Consent Requirements a Potential Harbinger for Adtech

The French data protection authority (CNIL) has closed its formal notice against a small France-based advertising company, Vectaury S.A.S. CNIL originally found that the company violated consent requirements under the GDPR by failing to obtain consent for the processing of geolocation data for advertising purposes. Importantly, CNIL's decision suggested that bundling consent might not be proper under the GDPR; specifically, the use of a single button on a website to grant free access to data controllers may be insufficient. The decision places advertising technology companies on notice that they need to pay close attention to their consent practices and implementations for obtaining appropriate user consent.

Read more at *TechCrunch* >>

Legislature, Attorney General Propose CCPA Amendments

California Attorney General Xavier Becerra has announced a bill intended to "strengthen and clarify" the California Consumer Privacy Act of 2018 (CCPA), including an amendment that would add a private right of action. This significant addition would give consumers the ability to enforce their new rights under the CCPA in court. The bill would also remove language that allows companies to cure CCPA violations before enforcement can occur, signaling Becerra's intention to enforce a zero-tolerance policy. Finally, in an effort to reduce taxpayer expenses, the bill would eliminate requirements that the attorney general's office provide businesses and private parties with individual legal counsel on CCPA compliance.

The California legislature also continues to propose amendments to the CCPA, including Assembly Bills 1202, 846 and 950. Assembly Bill 1202 would require data brokers to register and provide information to the California attorney general's office. Brokers who do not register may be subject to an injunction and civil penalties.

Assembly Bill 846 clarifies that consumers are not prohibited under the CCPA from choosing to participate in customer loyalty programs that offer incentives such as rewards, gift cards or other benefits. The proposed amendment further clarifies that businesses offering loyalty programs may continue offering benefits in a manner "reasonably anticipated" within the business-customer relationship context.

Assembly Bill 950 would require companies doing business in California and collecting consumer data on California residents to disclose the monetary value of the data. In order to comply with the provision, companies may publicly post the average monetary value of a consumer's data on their website. The proposed amendment also adds requirements for companies selling consumer data and establishes a Consumer Data Privacy Commission with the purpose of providing guidance for companies on how to appropriately determine the value of consumer data.

Washington State Inches Closer to Passing Consumer Privacy Act

Washington lawmakers held an open forum on February 27, 2019, regarding the Washington Privacy Act. Several key topics are still up for debate, including facial recognition and law enforcement

surveillance, the state attorney general's resources to adequately enforce the law, and the interaction with federal law. Various commenters welcomed the opportunity for Washington to have the "strongest privacy protections of any law in the U.S." by incorporating elements from the EU's GDPR regulation as well as the California Consumer Privacy Act while also improving on particular areas of existing laws. The bill is still in the committee process but will likely be introduced on the Senate floor in 2019.

Read IAPP's article >>

FTC Task Force Aims to Monitor Competition in Tech Markets

The Federal Trade Commission (FTC) has announced the creation of a task force "dedicated to monitoring competition in U.S. technology markets, investigating any potential anticompetitive conduct in those markets, and taking enforcement actions when warranted." The goal of the task force is "to closely examine technology markets to ensure consumers benefit from free and fair competition." The task force will be led by Patricia Galvan, currently the deputy assistant director of the Mergers III Division, and Krisha Cerilli, currently counsel to the director. The team will also include about 17 attorneys with unique expertise from various backgrounds.

Read the FTC's press release >>

Executive Order Significantly Alters Brazilian General Data Protection Regulation

An executive order has proposed several major changes to the Brazilian General Data Protection Regulation (LGPD), including the creation of a Data Protection National Authority and a Data Protection National Council. The order also removes the "natural persons" requirement, allowing companies, committees and working groups to be Data Protection Officers. Brazilian executive orders are effective immediately but "their conversion into law is conditioned to the assessment of the National Congress within a period of 120 days," according to the IAPP. The LGPD is scheduled to take effect in August 2020.

Read the IAPP's article >>

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**