March 2024

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

Hotel Chain Pays $12 Million to Resolve Privacy Violations

Motel 6 settled claims with the Washington State Attorney General for $12 million to resolve charges that Motel 6 violated the Consumer Protection Act and the Washington Law Against Discrimination. The lawsuit stems from a January 2018 lawsuit filed by Attorney General Bob Ferguson alleging that Motel 6 provided guests' private information to U.S. Immigration and Customs Enforcement without a warrant over a period of two years. The consent decree explicitly forbids Motel 6 from giving out guest information without a warrant or other lawful basis at every Motel 6 location in the United States. Specifically, the consent decree requires Motel 6 to properly train employees on how to handle and protect the personal information of guests. Motel 6 also agreed to seek approval of any policy or procedure from the Attorney General's Office as well as provide compliance records and reports to the Office for the next three years.

Read the press release and consent decree >>

Supreme Court Questions Standing in Privacy Cases

In an 8-1 decision, the U.S. Supreme Court ruled that Google could not move forward with its proposed $8.5 million settlement of a class action due to remaining questions regarding standing. The lawsuit stems from Google's practice allowing third-party websites to access users' search terms that could be used to identify users without their permission. After the Supreme Court initially accepted and decided the case, the Court expressed

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

concern about the issue of standing and remanded the case for the lower courts to address the standing issues.

Read the opinion >>

France Sets Boundaries for Biometric Information Use

The French data protection authority, CNIL, adopted regulations regarding the use of biometric information in the workplace. The "Model Workplace Biometrics Regulation" requires companies to set up a "biometric access control system" to comply with the new rule. Among the requirements, organizations must "justify the use of biometrics, by specific considerations (context, issues, specific technical and regulatory constraints, etc.) that are particularly detailed for the types of biometrics presenting the highest risk." Companies must also implement "rigorous specifications" with regard to "technical security measures" and "document the various choices made when setting up biometric devices."

Read the press release >>

Puerto Rico Drafts Digital Privacy Protection Law

The Puerto Rico Senate is considering a draft Law for the Protection of Digital Privacy that would provide consumers with the right to know what personal information is being collected and with whom it is being shared. The law would give consumers the right to opt out of the transfer, sale and sharing of personal information; would create a right of access, right to erasure and right to correct inaccurate or incomplete information; and would create a private right of action entitling the individual to seek $5,000 per violation.

The draft law would apply to any business that:

(1) collects personal information of Puerto Rico residents;

(2) determines the purposes and means of processing personal information; **and**

(3) (a) has a gross annual income exceeding $10 million;

(b) annually purchases, receives, sells or shares the personal information of 10,000 or more consumers for commercial purposes; **or**

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

(c) derives 20 percent or more of their annual income from the sale of consumers' personal information.

Read the draft bill >>

New Jersey Legislature Addresses Privacy Issues with Trio of Bills

The New Jersey General Assembly has passed a bill, SB 52, to amend the current breach notification law to require the disclosure of online account breaches. Specifically, provisions of the bill include adding "user name, email address, or any other account holder identifying information that, in combination with any password or security question and answer, would permit access to an online account" to the definition of personal information. The bill is awaiting the governor's signature.

Another bill, AB 4902, has been introduced in the state's Assembly Appropriations Committee. The bill "requires commercial Internet websites and online services to notify customers of collection and disclosure of personally identifiable information and allows customers to opt out." It also requires "an operator that collects the personally identifiable information of a customer to clearly and conspicuously post on its Internet website or online service homepage a link, entitled 'Do Not Sell My Personal Information,' to an Internet webpage maintained by the operator, which enables a customer to opt out of the disclosure of the customer's personally identifiable information." Furthermore, the bill "requires commercial Internet website and online service operators to notify customers of the collection and disclosure of personally identifiable information to third parties."

Lastly, AB 4974, which "requires operators of mobile device applications that collect user GPS data to notify users about how GPS data is disclosed and allow users to opt in to disclosure," has been reported out of Assembly Committee and will move forward in committees. In particular, the notification to a user must include, but is not limited to: 1) a complete description of the user GPS data that the operator collects through the mobile device application; 2) all third parties to which the operator may disclose user GPS data; and 3) the length of time the operator retains user GPS data.

Washington State Privacy Act Faces Significant Changes

After handily passing the Senate, the Washington Privacy Act is now facing some important changes by the Senate's counterparts

in the House. The proposed amendments include: (1) the potential for a consumer to bring an action against a controller if the state Attorney General refrains from acting on a consumer's written notice identifying allegations within 30 days; and (2) adding "publicly available information" to the definition of "personal data." Exemptions to the processing obligations added via amendment include "processing that is necessary for reasons of public health interest," "processing that is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes," and the safeguarding of intellectual property rights. The House version would apply to legal entities that "conduct business in Washington or produce products or services that are intentionally targeted to residents of Washington." The House Committee on Innovation, Technology & Economic Development passed the amended bill on April 3, 2019, and it now moves to the House Appropriations Committee.

Read the draft bill >>

Connecticut Becomes the Latest State to Consider the CCPA

The Connecticut legislature has introduced RB 1108, "An Act Concerning Consumer Privacy," which features language that essentially mirrors the original version of the California Consumer Privacy Act (CCPA). However, the bill does not incorporate any of the significant amendments made to the CCPA throughout the legislative process. Interestingly, the proposed legislation was introduced by the Joint Committee on Government Administration and Elections and has no individual sponsors. While the momentum of the bill is unclear, given the potential burden on businesses in Connecticut based on the significance of the CCPA on California businesses, this proposal is something to keep any eye on.

Read the draft bill >>

Pair of Texas Privacy Measures Move Forward

Two privacy bills have been introduced in the Texas House of Representatives. The Texas Consumer Privacy Act, HB 4390, echoes some of the same provisions of the CCPA, including the right of disclosure, the right to deletion, the right to know if certain personal information is being sold or disclosed, and the right to opt out of personal information being sold or disclosed by a business. Among other provisions, the Texas Consumer Privacy

Act defines "personal information" broadly as "information that identifies, relates to, describes, can be associated with, or can reasonably be linked to, directly or indirectly, a particular consumer or household." While the bill does not provide a private right of action, civil violations would range from $2,500 to $7,500 based on willfulness of the violator. If passed, the bill would take effect on September 1, 2020.

The Texas Privacy Protection Act, HB 4518, states that "a business shall develop, implement, and maintain a comprehensive data security program" as well as an "accountability program" that must include an annual assessment of privacy policies and procedures and the development of methods and procedures for responding to data breaches, among other obligations. Similar to its counterpart, the bill would not create a private cause of action. Civil offenses will not exceed $10,000 per offense and will not exceed a total of $1 million. Both bills are currently in committee.

New Zealand Focuses On Reducing "Notification Fatigue"

The New Zealand Parliament introduced an amendment to New Zealand's breach notification law that would raise the threshold for mandatory breach notifications. The bill proposes that individuals must be notified when "serious harm" is caused as opposed to the current standard of "harm." The factors used to determine what constitutes "serious harm" include: "the actions a holder of data has taken to reduce the harm; the sensitivity of the information; the nature of the harm; those to whom the information might be disclosed; and whether the information is protected by security measures." The bill, intended to address breach notification fatigue, still has a long road ahead before being signed by the Governor-General, but the proposal shows a significant policy shift by not requiring notifications in the event of minor data breaches.

Read the draft bill >>

Department of Commerce Issues Updated Privacy Shield Guidance

The Department of Commerce has updated its FAQ to address questions surrounding Brexit's effect on U.S. businesses complying with the Privacy Shield framework. The FAQ explains two scenarios in which Privacy Shield participants must update their Privacy Shield commitments by an "Applicable Date" depending on how the UK and the EU implement the withdrawal.

The first scenario applies a “transition period,” as agreed upon by the EU and UK, in which Privacy Shield participants can continue to receive personal data from the UK under the Privacy Shield until December 31, 2020. In the second scenario, there is no transition period and participants have until the date of the UK’s withdrawal from the European Union. In either case, after the Applicable Date, U.S. companies need to be aware of their obligations in order to continue receiving personal data from the UK.

Read the FAQs >>