March 2024

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

Shook's Tracking Tool for CCPA Amendments

Enactment of the California Consumer Privacy Act (CCPA) was the most notable event in years for U.S. privacy law. Now, a number of amendment bills are making their way through the California legislature, and Shook's Privacy and Data Security Team has been tracking those amendments closely. The team provides regular status updates via an easy-to-understand tracking tool and offers valuable insight regarding the progress of the amendments. Past updates have included:

- Explanation of the significant revisions to AB 25, one of the most-watched amendment bills, and how it went from modifying the definition of "consumer" to providing a time-limited exemption for personal information of employees, contractors and others.
- Notification of the failure of SB 561, which would have created a private right of action for any violation of the CCPA.
- A detailed rundown on which bills made it out alive from the California Senate Judiciary Committee's marathon hearing on July 9.

If you'd like to receive the CCPA Amendment Tracker, please contact Colman McCarthy.

French Data Protection Authority Issues Guidelines on Cookie Use

CNIL, France's data protection authority, has released new rules for obtaining consumer consent under the GDPR for companies using cookies and other tracking mechanisms. The updated guidelines replace CNIL's 2013 recommendations to align with

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 GDPR. Specifically, the new recommendations confirm that website operators must obtain valid consent before using tracking technology and that continuing past notice to merely browse the website is, alone, not enough for valid consent. CNIL will issue supplemental recommendations in early 2020.

TAKEAWAY

Companies governed by GDPR must ensure that their websites do more than simply provide notice of cookies and other tracking mechanisms. They must obtain valid consent, and ensuring they have a way to track or record consent is also advisable.

Equifax Settles Massive Security Breach Investigations

On July 22, 2019, Equifax reportedly reached a settlement agreement reaching up to $700 million with attorneys general from 48 states as well as the District of Columbia and Puerto Rico. The resolution comes two years after Equifax suffered an enormous data breach exposing the personal information of more than 147 million Americans. Investigations revealed that Equifax failed to follow basic cybersecurity principles by **not patching computer systems and storing sensitive data in plain text**, among other things. Equifax has agreed to set aside $425 million of the $700 million settlement to reimburse victims, settle claims with the Consumer Financial Protection Bureau for an additional $100 million and revamp its data security program, which is subject to audit for the next 20 years.

On the same day, Equifax settled a class action stemming from the same investigation. According to the terms of the settlement, Equifax has committed to "spend $1 billion on cybersecurity measures over the next five years and establish a $380.5 million fund to pay for four years of credit monitoring and financial help, where needed, in resolving identity theft issues for victimized consumers."

TAKEAWAY

The cost to businesses for "mega" breaches is well into the hundreds of millions or even billions of dollars.

New York Enacts Privacy Measures

Governor Andrew Cuomo has signed New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), which amended the state's breach-notification law. The Act, which takes effect March 21, 2020, amends the definition of personal information to include biometric information and online account

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

information and requires companies to implement reasonable safeguards to protect personal information.

Cuomo also signed the Identify Theft Prevention and Mitigation Services Act, which requires consumer credit-reporting agencies to offer—for free and for no longer than five years—identity-theft prevention and mitigation services to consumers who have been affected by a security breach of the agency's system. The law takes effect September 23, 2019.

At the local level, New York City lawmakers have proposed a bill that would make it unlawful for a mobile app developer or telecommunications carrier to share a customer's location data without an authorized purpose if the data was collected from the customer's device within the city. The bill broadly defines the term "share" as making "location data available to another person, whether for a fee or otherwise," suggesting that selling information is unlawful without an authorized purpose such as customer consent. The bill allows for a private right of action, including penalties for violations of $1,000 per violation, with a maximum penalty of $10,000 per day per person whose location data was unlawfully shared, as well as attorney's fees.

TAKEAWAY

Companies that collect personal information from New York residents should determine whether any of these changes affect them. Whether comprehensive privacy bills are passed, states continue to update their data-breach notification laws. These changes are primarily focusing on expanding the definition of "personal information" and trying to ensure some minimal steps are taken to secure personal information. Additionally, companies need to review their practices on collecting and using location data because an increasing number of laws are restricting the use of this type of personal information.

FTC Approves Settlement with Facebook

The Federal Trade Commission (FTC) announced a $5 billion fine against Facebook for failure to comply with a 2012 order related to its privacy practices. FTC's investigation largely originated from revelations about Cambridge Analytica's use of Facebook users' information, but the agency's new order also highlighted a number of other practices that violated the 2012 order. In addition to the fine, Facebook must **create an independent board-level committee to oversee and review its privacy efforts**, and its privacy practices will be subject to **review by an external assessor** to determine whether the company's practices comply with FTC's order.

The fine is the largest ever imposed by FTC—20 times larger than the previous world record for privacy and security violations. Facebook reported $55.8 billion in total revenue for 2018; **the $5 billion fine is 9% of that amount, much higher than the top potential fine under GDPR** (4% of revenue, or what would be about $2.23 billion for Facebook).

TAKEAWAY

By requiring board-level responsibility and external monitoring, FTC is signaling the importance of high-level oversight for privacy programs. These measures also show FTC's willingness to employ aggressive enforcement tools in the privacy sector.

Singapore to Certify Companies for Cross-Border Data Transfers

Singapore companies can now apply for certification to transfer data across borders in the Asia-Pacific region. Singapore's Personal Data Protection Commission announced that companies can achieve certification by showing that they meet criteria specified in the Asia Pacific Economic Cooperation's (APEC's) Cross Border Privacy Rule (CBPR) System or Privacy Recognition for Processors (PRP) Systems. Companies that demonstrate compliance will be able to more easily transfer data throughout the region, creating more business opportunities. The CBPR currently includes eight participating economies: United States, Canada, Japan, Mexico, South Korea, Australia, Chinese Taipei and Singapore. Of those, only the United States, Japan and Singapore offer mechanisms for companies to gain certification under the CBPR.

TAKEAWAY

APEC's CBPR system continues to grow in acceptance.

FTC Seeks Opinions on 2013 COPPA Amendments

In light of rapid technological changes, FTC is seeking comment regarding the effectiveness of amendments to the Children's Online Privacy Protection Rule (COPPA Rule). Originally, the 2013 amendments focused on how children use and access the internet as mobile devices and social networking become more accessible to them. The amendments expanded the definition of children's personal information to cover "persistent identifiers such as cookies that track a child's activity online, as well as geolocation information, photos, videos, and audio recordings." FTC is welcoming remarks regarding any provision of the COPPA Rule, "including its definitions, notice and parental consent

requirements, exceptions to verifiable parental consent, and safe harbor provision." Comments will be accepted until October 7, 2019.

TAKEAWAY

Companies that collect website information about children should review the amendments and may want to consider submitting comments.

SHOOK PRIVACY SPOTLIGHT

William "Bill" Sampson

With a list of awards nearly as long and deep as his experience, Bill Sampson has established himself as one of the country's premier litigators. He has tried more than 80 jury cases in federal, state, and military courts across a wide swath of practice areas. And, along with the over 100 programs he has taught to law students, clients and legal professionals, Bill brings that depth of experience and perspective to his privacy and data security practice. Beyond the many articles and presentations he has given on such subjects as standing in data-breach cases, legal and ethical risks in privacy and data security, and litigating data-privacy rights, Bill is a member of Working Group 11 of the Sedona Conference and currently chairs the Drafting Team charged with developing a legal test for whether reasonable security was used by the custodian of personal information.