January 2020

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

States Consider Privacy and Data Security Legislation

It's that time of year again, when we see a flood of legislative activity at the state level on privacy and data security laws. A couple of recent examples are below. Those interested in subscribing to Shook's state legislative tracker of privacy and data security laws should contact Colman McCarthy.

Florida House Bill 963 and SB 1670

Florida House Bill 963 and Senate Bill 1670 would make two important changes to Florida privacy law. First, it would prohibit companies from using personal information in public records requested from state agencies to market or solicit goods or services without first obtaining consent. (See this ABC interview with Shook Partner Al Saikali for an explanation of the issue the legislation is meant to address.) Second, the legislation allows consumers to opt out of the sale of their personal information by companies doing business online. It also requires companies doing business online to provide notice about their collection/use of consumers' personal information. The legislation would not create a private right of action. Saikali provides an in-depth analysis of the proposed legislation for corporate counsel at the *Data Security Law Journal*.

Virginia Senate Bill 641

Virginia Senate Bill 641 governs the sale of consumer data. The law would require companies to implement and maintain reasonable security procedures to protect the confidentiality of a consumer's data and ensure the accuracy of the data. Additionally, the law requires companies to allow consumers to opt out of the selling their personal data and must notify affected consumers in

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 event of a data breach. The attorney general may bring suit for $2,500 per unintentional violation and $7,500 per intentional violation. The law grants a civil cause of action for a consumer to recover up to $1,000 per violation in addition to any actual or punitive damages and allows for class actions.

Chicago's Data Breach Lawsuit Against Marriott Survives Motion to Dismiss

A court has rejected Marriott International, Inc.'s motion to dismiss the City of Chicago's data breach lawsuit filed in response to Marriott's data breach. Chicago's primary claim is that Marriott violated the city's consumer protection ordinance damaging Chicagoans who relied on safely inputting their information into Marriott's website. Additionally, the city asserts it has experienced a decline in revenue because residents and tourists refrain from staying at Marriott hotels operated in Chicago due to the breach. Marriott argued that Chicago's ordinance is preempted by the Illinois state constitution, but the court held that state lawmakers must explicitly include language in state laws to successfully preempt city ordinances. Chicago is seeking an injunction that requires Marriott to increase its data security safeguards and pay a fine of up to $10,000 for each day Marriott violated the ordinance.

TAKEAWAY

Chicago's lawsuit represents a successful example of a growing trend of municipalities taking action on behalf of their residents in privacy litigation.

UK Regulator Publishes Final Version of Children's Online Privacy "Code of Conduct"

The U.K. Information Commissioner's Office (ICO) has published its "Age Appropriate Design" Code of Practice, which sets forth 15 standards aimed at protecting children's online privacy. Organizations that provide online services "likely to be accessed by children in the UK" are required to, among other things, ensure that default privacy settings are set to "high," including switching off location settings and profiling tools allowing targeted content for those 17 and under. More generally, the Code requires that children's "best interests" be a primary consideration in the design and development of online services—regardless of whether those services are actually targeted to children.

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

Although the Code does not, on its own, create enforceable obligations, the standards laid out, if followed, will help companies offering online services in the United Kingdom ensure compliance with the special protection afforded children's data under the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Regulation (PECR**).** The ICO has stated that it intends to monitor conformance to the Code by way of proactive audits and that the failure to follow the Code will increase the difficulty of establishing that one's processing practices comply with the GDPR and the PECR.

The Code must now complete a statutory process and then be presented for Parliament's approval. Organizations will thereafter have a year-long implementation period in which to update their practices before the Code comes into full effect in or around fall 2021.

TAKEAWAY

GDPR-regulated companies that provide online services that children in the United Kingdom are likely to access should review the comprehensive Code and begin implementing its standards as soon as feasible. Failure to do so by 2021 could result in hefty fines of up to 4% of the companies' global revenue or 20 million euros, whichever is greater.

Company Settles FTC Violation for Misrepresenting Participation in the EU-U.S. Privacy Shield Framework

A California company settled U.S. Federal Trade Commission (FTC) allegations that it falsely claimed participation in the EU-U.S. Privacy Shield framework enabling the legal transfer of consumer data from EU countries to the United States. FTC alleged that the company falsely claimed it was a certified participant in the EU-U.S. Privacy Shield framework despite having only initiated an application with the Department of Commerce rather than completing all the steps to become certified. As part of the settlement with FTC, the company is prohibited from misrepresenting its participation in the EU-U.S. Privacy Shield framework, any other privacy or data security program sponsored by the government, or any self-regulatory or standard-setting organization.

TAKEAWAY

Be careful of statements in privacy policies. Always ensure that statements in privacy policies are true and accurate to avoid misrepresentation and potential liability.

Orbitz and Expedia Settle with Pennsylvania Attorney General in Payment Card Data Breach Lawsuit

Pennsylvania's Office of Attorney General has settled the Orbitz LLC and Expedia, Inc. payment card breach litigation, which allegedly exposed payment card information belonging to Pennsylvania residents. The settlement ($110,000) includes $80,000 for civil penalties and requires Expedia and Orbitz to increase their security safeguards by:

- Implementing a comprehensive information security program on the Orbitz website;
- Conducting an annual comprehensive risk assessment;
- Developing a plan and program for designing, implementing and operating safeguards;
- Performing regular security monitoring, logging and testing;
- Employing improved access control and account management tools;
- Reorganizing and segmenting its network; and
- Complying with Payment Card Industry Data Security Standards.

TAKEAWAY

Regulatory actions based on data breaches are a mainstay in data privacy and security litigation. Companies should implement and *continuously* maintain security safeguards.

Google Wins Motion to Dismiss Class-Action Complaint Regarding User Location Tracking

A California federal court granted Google's motion to dismiss a class-action complaint alleging that Google violated California's Invasion of Privacy Act (CIPA) by illegally tracking and storing users' private location information without consent. Google argued that users consented to Google's collection of their location information when they agreed to Google's terms of services and that they implicitly consented by using Google's services. The court dismissed the plaintiffs' CIPA claims with prejudice but allowed them to amend their claims that Google's data collection violated California's state constitution and common law right to privacy.

TAKEAWAY

Review terms of service to confirm they accurately explain information collection and use practices, then ensure proper recording of consumer consent. It may also be useful to conduct periodic audits.

Equifax Settles Claims Stemming From 2017 Massive Data Breach

The Northern District of Georgia approved a settlement in a class action stemming from the 2017 Equifax data breach that affected approximately 147 million consumers. Under the settlement, Equifax will pay $380.5 million to settle lawsuits stemming from the 2017 data breach and will reserve an additional $125 million for potential out-of-pocket claims by consumers. Class members will receive 10 years of credit monitoring or the equivalent cash compensation if the consumer already has credit monitoring. Additionally, Equifax will pay at least $1 billion for improving its privacy and security practices plus significant litigation and attorneys' fees.