March 2024

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

The California Consumer Privacy Act: The Next Frontier

The California Consumer Privacy Act (CCPA) has been called the beginning of America's GDPR. As the most comprehensive privacy law in the United States, entities doing business in California need to ensure they are in compliance or risk severe penalties. In a white paper, "The California Consumer Privacy Act: What Every In-House Lawyer Should Know," Shook Partner Al Saikali provides in-house lawyers with a comprehensive guide that covers the CCPA's scope, requirements and tips on operationalization. Saikali also recorded a webinar on the CCPA's requirements with Of Counsel Steve Vieux and Associate Colman McCarthy that can be accessed at any time.

HHS Lowers Cumulative Annual Limits for HIPAA Violations

The U.S. Department of Health and Human Services (HHS) has issued revised monetary-penalty limits for Health Insurance Portability and Accountability Act (HIPAA) violations by covered entities. Under the revisions, the maximum annual penalty for violations per tier of culpability would be:

Culpability	Old Annual Limit	New Annual Limit
No Knowledge	$1,500,000	$25,000
Reasonable Cause	$1,500,000	$100,000

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

Willful Neglect – Corrected	$1,500,000	$250,000
Willful Neglect – Not Corrected	$1,500,000	$1,500,000

While each tier is capped, an entity can violate multiple tiers depending on the circumstances of violation. Accordingly, the Office of Civil Rights (OCR) can issue penalties up to the annual limit for more than one tier.

TAKEAWAY: The revised monetary-penalty limits are consistent with the decreased enforcement activity we have seen from the OCR in the last few years.

Read the HHS Notification and FAQs >>

Washington State Privacy Act Expires but Legislature Passes Breach Notification Law

Senate Bill 5376, the "Washington Privacy Act," has deteriorated after the House failed to vote on the bill during the current legislative session. The bill would have created a comprehensive privacy law for Washington similar to the California Consumer Privacy Act. The bill, which passed the Senate unanimously, faced stiff opposition in the House and failed to get through the committee process. Further attempts to pass the bill will have to await the next legislative session.

Additionally, House Bill 1071, requested by Washington State Attorney General Bill Ferguson, shortens the deadline to notify individuals of a data breach from 45 days to 30 days. The Washington Attorney General's office must also be notified within 30 days of the discovery of the breach. The bill also expands the definition of "personal information" to include an individual's name along with any one of the following: full birth dates, health insurance ID numbers, medical history, student identification numbers, military identification numbers, passport identification numbers, usernames and passwords, biometric data (such as DNA profiles or fingerprints), and electronic signatures. The Washington legislature passed the bill on April 15, 2019, and it awaits the governor's signature.

TAKEAWAY: We do not have cause for concern (for now) about a comprehensive privacy law coming from the state of Washington, though companies that suffer a breach affecting Washington

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

residents should be aware of the recent changes to the state's breach notification law.

View the House Bill and the Senate Bill >>

North Carolina Introduces Amendments to Data Privacy Law

The North Carolina legislature has introduced amendments to its Identity Theft Protection Act. The provisions of House Bill 904 detail many notable changes, including a 30-day data breach notification period and an obligation of an organization to offer free credit monitoring services for a minimum of two years if the breach affects an individual's Social Security number. Additionally, the definition of personal information would be expanded to include "[h]ealth insurance policy number[s], subscriber identification number[s], or any other unique identifier[s] used by a health insurer or payer to identify [a] person" and "any information regarding the individual's medical history or condition, medical treatment or diagnosis, or genetic information, by a health care professional." Furthermore, the definition of "security breach," as proposed, would include "any determination that illegal use has not occurred or is not reasonably likely to occur or that no material risk of harm is created shall be documented and maintained for at least three years." The bill has passed the first reading in the House and will be debated as it moves through the process.

TAKEAWAY: There is a new trend to *require* that credit monitoring be offered in some states where certain personal information is affected by a data breach. We are also seeing states broaden the definition of personal information.

View the bill >>

Marketing Company Hit with $925 Million TCPA Verdict

A jury has awarded a class of consumers $925 million in damages in a class action alleging marketing company ViSalus engaged in a marketing campaign that initiated robocalls without consent. Following a three-day trial, the jury found that ViSalus had made 1,850,436 calls violating the Telephone Consumer Protection Act (TCPA). Statutory damages set a penalty of $500 per violation, but the judge must still officially rule on the damages award.

TAKEAWAY: The penalties for violating the TCPA can be massive. Companies should assess whether the law applies to their

organizations and whether they have a process in place to ensure compliance.

Read more at *The Oregonian* >>

University Settles $4.7 Million Lawsuit Following Theft of Hard Drive

Washington State University settled a lawsuit for $4.7 million after an unencrypted portable hard disk drive containing the personal information of approximately 1.2 million people was stolen from a storage unit where the university's research center stored periodic backups. Among the numerous settlement terms, the university agreed to include two years of credit monitoring for individuals whose information was exposed; conduct a data-security assessment to implement necessary policies, procedures, training and technology; move research backup drives to secure locations; and pay administrative and attorneys' fees.

TAKEAWAY: Encrypt! Encrypt! Encrypt!

Read the decision >>

Polish Data Protection Agency Issues First GDPR Fine

Bisnode, a European digital marketing company with an office in Poland, was hit with a €220,000 fine after Poland's data protection authority found that the company did not obtain proper consent to process individuals' data because although Bisnode used software to crawl and extract data from publicly available internet sources, it did not directly obtain consent from any individuals to process their data. Although the fine itself is fairly small, Bisnode was also ordered to contact the 5.7 million individuals affected by the violation, which the company estimates will cost approximately €8 million.

TAKEAWAY: Companies collecting publicly available information over the internet may be subject to fines under the GDPR if they do not obtain proper consent from the individuals whose data they collect.

Read more at *TechCrunch* >>

Algorithmic Accountability Act of 2019 Introduced in U.S. Congress

Sens. Cory Booker (D-N.J.) and Ron Wyden (D-Ore.) have introduced Senate Bill S.1108, the "Algorithmic Accountability Act of 2019," which would require "entities that use, store, or share personal information to conduct automated decision system impact assessments and data protection impact assessments." Entities affected would include any person, partnership or corporation over which the Federal Trade Commission (FTC) has jurisdiction under Section 5(a)(2) of the FTC Act and that meet certain other thresholds. The assessments would require evaluating the design of automated decision-making systems and their potential accuracy, fairness, bias, discrimination, privacy and security. Further regulatory action from FTC would be required within two years of the date of enactment.

TAKEAWAY: Companies that use or are considering using personal information to make automated decisions should monitor the progress of this legislation.

View the bill >>

Medical Imaging Service Settles $3 Million HIPAA Violations

Touchstone Medical Imaging, a Tennessee-based diagnostic medical imaging service, settled alleged HIPAA violations for $3 million as a result of a breach exposing patients' personal health information (PHI). In 2014, the FBI and OCR notified the company that one of its FTP servers was accessible to the public, allowing anyone to connect to a shared directory that contained the PHI of patients. OCR's investigation revealed that the PHI of more than 300,000 patients was exposed, including "names, birth dates, social security numbers, and addresses." Additionally, OCR found that Touchstone missed the individual breach notification deadline by failing to conduct a proper investigation and "failed to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of its ePHI." Touchstone has agreed to "undertake a robust corrective action plan that includes the adoption of business associate agreements, completion of an enterprise-wide risk analysis, and comprehensive policies and procedures to comply with the HIPAA Rules."

TAKEAWAY: Companies should be performing regular penetration tests to ensure that their servers and databases are not making sensitive information publicly accessible.

View the HHS Press Release and Resolution Agreement >>

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