Four Key Developments in Data, Data Protection and Cybersecurity Law

By: Kevin D. Pomfret

03.25.2022

The month of March has seen significant developments in the cybersecurity and data protection space. Here are four key legal developments that could be critical to your business.

President Biden Signs Law that Requires Certain Companies to Disclose Cyber Incidents

On March 15, President Biden signed the Consolidated Appropriations Act of 2022 (the ?Appropriations Act?), which funds the federal government until September 2022. The Appropriations Act included the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (the ?Critical Infrastructure Act?).

Under the Critical Infrastructure Act, covered infrastructure entities will be required to:

- report to the U.S. Cybersecurity and Infrastructure Security Agency (CISA) any ransomware payments within 24-hours; and
- report to CISA within 72-hours all covered cyber incidents.

However, these requirements will only take effect upon the issuance of implementing regulations from the Director of CISA. These implementing regulations will be critical as they will need to identify which critical infrastructure entities are covered and which cyber incidents are reportable.

California Attorney General Opinion Requires Companies to Disclose Internally Generated Inferences

On March 10, the California Attorney General issued an opinion regarding the obligations of companies subject to the California Consumer Privacy Act (the ?CCPA?) to disclose, upon consumer request, certain internally generated inferences about them. Specifically, the opinion states that under the CCPA a consumer has the right to request internally generated inferences about them if such inferences are both (i) derived from information that is otherwise considered personal information under CCPA, and (ii) used by the business to create a profile about that consumer. There are several statutory exceptions to

this disclosure requirement. In addition, companies are not obligated to disclose trade secrets.

SEC Proposes Reporting Requirements for Cybersecurity Incidents

The Securities and Exchange Commission decided on March 9 to propose a rulemaking that would impose a number of new requirements on public companies, including a 4-day reporting requirement for U.S. companies that have experienced a "material cybersecurity incident.? This Form 8-K disclosure would include, to the extent known:

- when the incident was discovered;
- whether it was ongoing;
- a brief description of its nature and scope;
- whether any data was stolen, altered, accessed, or used for any other unauthorized purpose;
- the effect of the incident on operations; and
- whether the company "has remediated or is currently remediating the incident."

FTC Requires Another Company to Delete Algorithms

On March 3, the Federal Trade Commission (FTC) announced that it had reached a settlement with WW International, Inc., formerly known as Weight Watchers, for violations of the Children?s Online Privacy Protection Act (COPPA). Specifically, the company had actual knowledge that it had collected personal information from minors under the age of 13 without the consent of the minors? parent. The settlement order requires WW International to:

- pay a $1.5 million penalty;
- delete personal information collected from children; and
- destroy any models and algorithms derived from the improperly collected data.

Data is a critical component in developing the models and algorithms that are driving machine learning and artificial intelligence. The settlement is another example of the FTC?s efforts to ensure that companies do not benefit from improperly collected data after the data has been deleted. It follows a similar 2021 settlement with Everalbum, Inc. which required the company to not only delete the photos and videos of app users but also the models and algorithms it developed by using those photos and videos.

Stay tuned for more legal developments related to data management, including privacy and data protection, cybersecurity, intellectual property rights and data quality. Please contact **Kevin Pomfret** (703.760.5204 | **kpomfret@williamsmullen.com**) with any questions.

Related People

- Kevin D. Pomfret ? 703.760.5204 ? kpomfret@williamsmullen.com

Related Services

- Data Protection & Cybersecurity