DAVIS GILBERT

Data Security Legislation Is on the Rise — Marketers and Their Agencies Must Be Vigilant About Their Controls

6th Edition: Trends in Marketing Communications Law

2018 saw a surge of state data security legislation, including by Alabama, Arizona, California, Colorado, Iowa, Louisiana, Nebraska, Ohio, Oregon, South Carolina, South Dakota, Vermont and Virginia. These laws are intended to enhance and strengthen existing data protection guidelines and, in some cases, are modeled after existing standards, such as the European Union's General Data Protection Regulation. These new (or amended) regulations set minimum data security requirements and practices for businesses that collect and process personal data. Additionally, they identify breach notification time periods, broaden the definitions of "personal information" and add safeguards with regard to the information of minors. Other notable changes include, in the case of Colorado and Nebraska, requirements to flow down appropriate security measures to service providers receiving personal information.

While all 50 states have now implemented general data breach notification laws, a few states went further to add sector-specific laws in 2018. In order to provide more transparency to consumers regarding the collection and use of their information, Vermont passed a new law that imposes on data brokers certain minimum data security standards, breach disclosure obligations and a yearly registration requirement with the Vermont Secretary of State. South Carolina's new Insurance Data Security Act also reflects this trend, requiring state licensed insurance companies to implement comprehensive written cybersecurity programs.

The Ohio Data Protection Act (Ohio Act), described as the "first-of-its kind," provides any business that has suffered a data breach with a safe harbor to limit exposure to litigation if the business can show that it maintained and complied with an "appropriate" cybersecurity program at the time of the breach, taking into account multiple factors, including the size, complexity and nature/scope of the business's data processing activities.

However, states are not the only bodies paying attention to the need for better data security practices. The National Institute of Standards and Technology has also updated its existing "Cybersecurity Framework" (Framework) and released a "Roadmap" to accompany the Framework, in order to clarify the requirements that make up the Framework, while also allowing for some flexibility in its implementation. Although the Framework is not law, it is generally accepted as a streamlined tool to manage the risks and threats inherent to an organization's cybersecurity. As these threats continue to evolve (and grow in importance with ever-greater reliance on technology), lawmakers are increasingly looking to the Framework and other industry standards and best practices for guidance in crafting their respective recommendations. Notably, adherence to the Framework and other standards is cited by the Ohio Act as one element of qualifying for the safe harbor.

Although not yet uniform, a common theme in data security legislation has been the requirement to implement an internal security program with appropriate safeguards, which would benefit marketers and consumers alike.

Key Takeaways

- Data security is a growing priority to U.S. lawmakers.
- Covered organizations must remain diligent in their compliance efforts, bearing in mind the various laws and regulations that may apply.
- An appropriate information security program must take into account the type of data and related processing activities.

Related People

Gary Kibel
Partner
212 468 4918
gkibel@dglaw.com

Oriyan Gitig
Counsel
212 468 4880
ogitig@dglaw.com