AS STATES AND NATIONS CONTINUE TO ENACT COMPREHENSIVE DATA PRIVACY LEGISLATION, PRESSURE MOUNTS ON THE U.S. TO PASS A COMPETING FEDERAL LAW IN 2021, AND BUSINESSES SHOULD PREPARE FOR COMPLIANCE

PUBLICATION - JORDAN KOVNOT, CHASE J. WRIGHT, SEPTEMBER 10, 2021

Global data privacy legislation has steadily advanced over the past several years, with one of the most comprehensive and well-known laws being the General Data Protection Regulation (GDPR), governing personal data originating in the European Union, which went into effect in 2018. Many other countries, such as Brazil, Japan, and Australia, have followed suit and enacted similar legislation to regulate industries and protect certain rights of consumers, businesses, and other parties that are affected in their respective territories. China, on a similar path, released draft legislation, the Personal Data Protection Law (PDPL), late in 2020 that is moving towards passage. The United States, however, still lacks a comprehensive law at the federal level, relying instead on a patchwork of state laws to protect data privacy rights in the U.S., resulting in confusion across states and costly compliance for U.S. businesses.

Although all of the fifty states, as well as the District of Columbia, Puerto Rico, Guam and the Virgin Islands, have enacted some form of data breach notification or data protection laws, they differ significantly in applicability, scope, enforcement, and penalties. This inconsistency in state laws has resulted in the need for robust analysis of applicable state policies and added expense for U.S. businesses to ensure compliance for those that collect, process, or otherwise handle personal data (which in today's environment is almost everyone) as well as adding to the cost and confusion of responding to a potential data breach scenario.

STATE APPROACHES

The most comprehensive legislation that has been passed in the U.S. to date is the California Consumer Privacy Act (CCPA), which went into effect in 2020 and overlaps with the GDPR in many respects. Some of the mandates that we would expect in any comprehensive federal legislation would likely piggyback off of those protections afforded in the CCPA, such as: (1) a consumer's right to know how their personal information is collected, used, and shared; (2) the right to delete certain personal information that businesses collect; and (3) the right to opt-out of the sale of their personal data.

Since the CCPA was enacted, other states have followed California's lead and many have used the CCPA as a template in crafting its own state laws and regulations. In March 2021, Virginia joined California as the second state to pass a comprehensive consumer privacy law, the Virginia Consumer Data Protection Act and offers Virginia residents some CCPA-like rights to access, correct and delete their personal data, as well as a right to opt-out of sales of personal data. In July 2019, New York passed the Stop Hacks and Improve Electronic Data Security Act

(the "SHIELD Act") which updates New York's breach notification procedures and requires businesses to implement reasonable physical, technical, and administrative safeguards such as internal monitoring, training, and data disposal methods.

However, even the landmark CCPA will soon be out of date, as California subsequently passed new legislation, the California Privacy Rights Act (CPRA), which is set to go into effect on January 1, 2023. The CPRA is expected to toughen certain aspects of the CCPA and bring the state law even more in line with the GDPR.

Now that we are nearly three years from the initial passage of the CCPA and enactment of the GDPR, many in the U.S. are lobbying for comprehensive data privacy legislation at the federal level that would bring uniformity and govern all fifty states and U.S. territories.

ADVANTAGES OF A FEDERAL LAW

The benefits of having a federal law are numerous. Foremost, federal data privacy legislation would make clear to consumers which baseline rights they are entitled to when it comes to safeguarding their privacy and personal data and ensure there are appropriate enforcement mechanisms in place, rather than requiring consumers to parse through privacy policies and understand the nuances of various state laws (some of which provide relatively weak protections).

In addition to consumer rights, businesses will also benefit from comprehensive legislation at the federal level. A federal law would provide a streamlined framework for business compliance and allow businesses to better grasp and observe data privacy requirements, as opposed to monitoring fifty separate state laws and attempting to analyze, interpret, and build frameworks that comply with each.

Additionally, the compliance itself can also add a new level of value to businesses. By conforming to a comprehensive data privacy law, businesses are forced to grapple with (and better understand): (1) the type of data that they possess, (2) their rights and capabilities with respect to the data, (3) how to better protect their customer's (and their own) personal data, (4) the internal data protection standards and protocols they have in place, and (5) overall organizational risk with respect to data use, protection, and security.

A STARTING POINT IN CONGRESS

Starting in 2019 and throughout 2020, competing federal bills have increasingly been introduced in the U.S. Congress, showing the need for uniform legislation and momentum for a possible law later this year. The *Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act* was introduced in 2020 by Senators Wicker, Thune, Fischer, and Blackburn. This bill followed the *Data Protection Act of 2020* introduced by Senator Kirsten Gillibrand, the *Consumer Online Privacy Rights Act of 2019 (COPRA)* introduced by Senators Cantwell, Schatz, Klobuchar, and Markey in December of 2019, and several other

bills sponsored by both Democrats and Republicans.

An April 2020 report by the Congressional Research Service details that these bills all share common principles of creating a conglomerate of rights to protect consumer's digital privacy. The bills tend to diverge on individual rights of action against businesses and whether the legislation would preempt state laws.

The most recent bill, the *Information Transparency and Personal Data Control Act (ITPDCA)*, was introduced in March of 2021 by Representative Suzan DelBene, a former Microsoft executive. The ITPDCA contains the broadest of concepts found in prior bills and is seen as the most likely for bipartisan support, but, unless traction is gained, the Democrat-sponsored COPRA is currently seen as the strongest for potential passage with Democrats controlling the House, Senate, and White House.

Regardless of any action in Congress, the Biden Administration has focused the attention of the Federal Trade Commission (FTC) to push for more aggressive data protection regulations, which should continue to be monitored. The FTC has frequently interpreted its authority to regulate "unfair and deceptive trade practices" under the FTC Act to target companies that fail to reasonably protect the security of customer's personal information. Federal courts have upheld the FTC's authority to regulate data security practices in this way, as was displayed in *FTC v. Wyndham Worldwide Corp.* (799 F.3d 236 (3d Cir. 2015)).

BUILDING THE FRAMEWORK FOR COMPLIANCE TODAY

While state and federal laws and related guidance continue to evolve, it is apparent that these privacy protection requirements will continue to expand in the U.S. and abroad in the coming months and years. Businesses should prepare for compliance now as a way to have an organizational foundation and framework to build upon as new regulations on the use of data and technology become increasingly inevitable. As an example, even more pioneering legislation was announced in the European Union on April 21, 2021, governing the use of artificial intelligence (AI), which is the first policy of its kind that governs how businesses can use this rapidly expanding technology.

Even as the U.S. continues to negotiate a federal law, businesses should stay informed and be proactive. Any legislation that is passed in the U.S. will certainly have components of the GDPR, CCPA, CPRA, other state laws, and possibly incorporate AI or other areas of privacy and consumer protection. One thing is certain, compliance with such frameworks today will prepare for a more seamless transition when a comprehensive law is eventually enacted in the U.S.

PROFESSIONALS

Jordan Kovnot

Chase J. Wright