The U.S. Approach to Privacy: What Is It, and Where Is It Headed?

Aaron J. Burstein, Alyssa Z. Hutnik

January 28, 2020

As we mark Data Privacy Day, today is a good time to take stock of where U.S. privacy legislation stands in relation to the developments of the past few years. In less than two years, the GDPR and the CCPA became the most comprehensive privacy laws in effect, granting individuals extensive rights over their information, creating numerous accountability requirements, and giving authorities the power to impose potentially massive fines. (For more information on the GDPR, see our blog posts, including those here and here.)

The CCPA ignited a debate about whether it rejects or maintains the "American approach" to privacy. Some observers panned the CCPA for departing from the "American approach" of "largely permissionless innovation with a post hoc regulatory response to concrete [privacy] harms." Others criticized the CCPA for generally allowing personal data collection and use unless prohibited by a "specific legal rule."

This debate is unlikely to be resolved soon or conclusively, but it is clear that at the federal and state levels, U.S. data privacy laws are likely to expand. While some states – including Washington and Virginia – are considering GDPR-influenced comprehensive bills, states also continue to consider and add laws that address specific data practices, which could cause further fragmentation in U.S. privacy laws and additional compliance challenges for companies.

How should companies manage the uncertain path that privacy legislation is following in the U.S.? Taking a comprehensive, holistic look at an organization's data practices is often key to complying with current requirements (such as the CCPA) and also is likely to be an effective way to manage disparate state laws as they develop.

Toward Comprehensive State Privacy Laws

The GDPR has had an important impact on global privacy laws. Argentina, Brazil, Malaysia, and Uruguay, among others, have adopted privacy laws modeled after the GDPR. The CCPA includes several GDPR elements, such as the rights to access and to deletion, though significant differences remain. (For a more granular look at how the GDPR and CCPA compare, see our comparison chart here.) In addition, Washington state legislators are currently pushing for a Washington Privacy Act (SB 6281), a new regulation governing data privacy and facial recognition. The bill explicitly references the GDPR, stating, "The European Union recently updated its privacy law through the passage and implementation of the general data protection regulation, affording its residents the strongest privacy protections in the world. Washington residents deserve to enjoy **the same level of robust privacy safeguards**" (emphasis added). Virginia similarly is considering privacy legislation that would give consumers the right to access their data and determine if it has been sold

to a data broker (HB 473). Virginia's bill would generally track the GDPR consumer rights, including the rights to access, correction, erasure, and the right to opt-out of further processing.

The Differences: An Example

Other aspects of the "American approach" to privacy are holding fast against the movement toward comprehensive laws. Biometric privacy exemplifies the differing approaches of the EU and U.S. In the EU, biometric data falls under the GDPR as a "special category of personal data," and companies must not process this data unless they obtain explicit consent, or the processing meets other stringent grounds for lawful processing that apply across all EU member states. Also as part of the GDPR, any unauthorized access to or acquisition of biometric data that constitutes a data breach must be reported to the relevant authority within 72 hours.

In the United States, biometric privacy is a state law issue (for now), complemented by a handful of enforcement orders that address biometric data. Only three states have relevant laws on point – Illinois, Washington, and Texas – and the scope of and requirements under these laws vary considerably. For example, biometric information may trigger data breach notification obligations if it is compromised, but whether the obligations are triggered will vary from state to state. An important distinction also lies in enforcement capabilities – Illinois's biometric law has a private right of action, whereas the Texas and Washington laws do not. Additionally, laws such as HIPAA and Title VII may provide additional protections in some situations.

Outside of the U.S. and EU, countries are following Europe's lead. Very few countries have specific laws that govern biometric data, and instead include this data under a national law, which often contains informed consent requirements and data subject rights. While questions remain about how protective this approach is where biometric data is concerned, very few countries are addressing these questions through laws that apply to sectors or territories.

The Implications: A Conversation

While the EU approach to privacy seems to be winning globally, U.S. policymakers are not ignoring more targeted requirements that address specific data practices. However, this piecemeal approach could also cause confusion, complexity, and expense. For example, the CCPA's "Do Not Sell My Personal Information" requirement could quickly become impractical if states were to adopt different definitions of "selling" personal information.

Members of Congress who are considering a federal privacy bill have the chance to decide how much of the U.S. approach and how much the EU approach to put into any comprehensive federal law protecting personal information, as well as whether to include preemption and a private right of action. We will be watching closely to see how they decide.

At bottom, this is just the beginning for data privacy laws. Consumer data rights, governance and accountability requirements, and regulatory structures will surely evolve and likely expand. For companies attempting to build some future-proofing into their privacy programs, taking the time to understand their data practices, what types of personal information they collect and maintain, where it is, why and how long they need it, and whether the personal information is sufficiently protected against compromise will enable more options for business strategies as well as more efficiently manage enterprise risk in response to the changing legal landscape.


THE NEW ADVERTISING AND
PRIVACY RESOURCE CENTER
Advertising, Privacy and Consumer
Protection Answers. All in One Place.
CLICK HERE FOR MORE INFORMATION