

CCPA Update: California Public Forums and Other Proposed State/Federal Legislation

The Bottom Line

- *Taken together, these legislative developments are indicative of the increasingly complicated and potentially confusing data privacy regime that lies ahead.*
- *What remains clear is that businesses that process personal information need to remain diligent about privacy and data security compliance in this rapidly changing landscape.*

The California Consumer Privacy Act (CCPA), a comprehensive state privacy law that was passed and subsequently amended in 2018, is continuing to raise questions for businesses operating in California. Under the recent amendments, the California Attorney General will not begin enforcing the CCPA until the earlier of six months after the Attorney General issues implementing regulations or July 1, 2020, though the law does become effective January 1, 2020.

In January, to further the rulemaking process, public forums were held as part of the Attorney General's preliminary diligence and inquiry into public sentiment regarding the CCPA. Not to be outdone, other lawmakers, at both the federal and state level, have been introducing their own privacy bills, seemingly at an even faster pace.

CCPA Public Forums

The purpose of the public forums is to allow public participation in establishing regulations that will provide businesses with guidance regarding compliance with the CCPA. Seven key topics have been identified as the focus of these forums, including:

- Updates to categories of personal information;
- Updates to the definition of unique identifiers;
- Establishing exceptions to the CCPA to enable businesses to comply with other state and federal laws;
- Rules for handling consumer opt-out requests;
- Development of a uniform opt-out logo and button;
- Rules to ensure privacy notices are easily accessible and understood; and
- Rules for verifying consumer requests.

In January, the first two of these forums were held in San Francisco and San Diego. Among other things, participants at the forum asked for clarifications on definitions including "Personal Information," "Business," "Consumer," and "Sale." Several speakers requested safe harbors for businesses that are GDPR compliant

and/or those that use template privacy notices prescribed by the Attorney General. Others expressed concerns about how the CCPA would apply to loyalty programs and targeted advertising. Additionally, requests were made for guidance around the notice, access and opt-out requirements.

One commenter suggested that a company's cyber security preparedness should be considered in determining presumption of liability in the event of a data breach. The advertising industry is particularly interested in resolving these issues, since a literal reading of the law could significantly disrupt the current practices, such as behavioral advertising.

Although many questions were raised, no feedback has yet been provided. In addition to the seven forums currently scheduled, the public has also been encouraged to submit written comments to the Attorney General's office through the end of February. In short, it looks like it may take some time before the Attorney General will provide the clarifications that California businesses are eagerly awaiting.

Other Proposed Legislation at the Federal and State Levels

While eyes have been focused on California and the CCPA, lawmakers across the country have been introducing other privacy bills to address similar concerns around data privacy. Key among these are the American Data Dissemination Act, the Social Media Privacy and Consumer Rights Act of 2019, The Washington Privacy Act and New York's Right to Know Act of 2019.

American Data Dissemination Act

In response to the growing pressure to address consumer data privacy issues, Senator Marco Rubio introduced a national data privacy bill, called the American Data Dissemination Act (ADDA), which would preempt state privacy laws, such as the CCPA. Under the ADDA, the FTC would be required to submit detailed recommendations for privacy rules for review by Congress. In turn, Congress would then have the power to draft a national privacy law, which would replace the current patchwork of state laws. The hope is that the federal law would simplify the increasingly complex data privacy and security compliance framework facing companies today.

Social Media Privacy and Consumer Rights Act

U.S. Senators John Kennedy and Amy Klobuchar also recently reintroduced their Social Media Privacy and Consumer Rights Act. The bipartisan bill seeks to make it easier for consumers to understand how their data is used and would enable consumers to opt out of certain data tracking and collection processes. The bill also contains data breach notification requirements.

The Washington Privacy Act

On the heels of California, and in anticipation of the continued success and growth of its technology sector and associated flow of consumer data, Washington legislators have introduced a robust privacy bill (scheduled to go into effect in December 2020) known as the Washington Privacy Act (WPA) that provides Washington residents with data and privacy protections similar to that of the EU's GDPR.

The WPA would apply to: (i) companies that process the data of more than 100,000 Washington residents and (ii) data brokers that derive greater than 50% of gross revenue from the sale of personal information and process the data of more than 25,000 Washington residents.

Exempted are businesses that are already subject to certain other federal privacy acts. In addition to other controls and protections, the WPA is intended to give residents greater control over the processing of their personal data (including with respect to their right to access and update data, data portability and object to use of their data). The WPA also includes data security assessment requirements. As with other pending state privacy laws, the state Attorney General would be responsible for enforcement.

Right to Know Act of 2019

New York's legislature is currently considering a privacy bill known as the Right to Know Act of 2019, to provide consumers with more transparency and control over the collection and use of their personal information. Consistent with other pending privacy legislation, the Right to Know Act requires that consumers be provided with access to their data. Furthermore, businesses would be required to make available to data subjects information regarding the categories of their personal information disclosed to third parties, as well as the identity of any such third parties. The bill's definition of "Personal Information" is notable in that it broadly includes information that identifies or can be associated with either an individual or an electronic device. Both consumers and the state Attorney General would have the right to bring a civil action to recover damages.

Related People

Richard S. Eisert

Partner/Co-Chair Advertising + Marketing

212 468 4863

reisert@dglaw.com

Gary Kibel

Partner

212 468 4918

gkibel@dglaw.com

Oriyan Gitig

Counsel

212 468 4880

ogitig@dglaw.com