Published on *The National Law Review* https://natlawreview.com

GDPR in the USA? New State Legislation Is Making This Closer to Reality

Article By:

Bryan Clark

The European Union's General Data Protection Regulation ("GDPR") is well known as the toughest privacy and security law in the world, as it has a wide reach and imposes heavy fines against those who violate its privacy and security standards (which are quite broad). The impact of the GDPR has already been felt in the United States since it went into effect in 2018, and now U.S. lawmakers in numerous states are moving to enact similar legislations. The California Consumer Protection Act ("CCPA") was the first instance of the GDPR's impact in the United States, as California put in place a statute and regulations that mirrored theGDPR in several respects. Now Virginia has set in motion what could be a year-long string of states enacting similar legislation. In particular, Washington and New York have proposed legislation following the framework of the CCPA. This article will compare the CCPA to the newly enacted and proposed privacy laws in the United States.

Newly Enacted and Proposed Privacy Acts:

Newly Enacted Virginia Act

On March 2, 2021, Virginia passed its Consumer Data Protection Act ("CDPA"), the second comprehensive consumer data privacy law in the United States. The CDPA will go into effect on January 1, 2023. The CDPA applies to persons or entities that conduct business in Virginia or produce products or services offered to Virginia residents and that "control or process" personal data. The Act applies to businesses that (1) control or process personal information of at least 100,000 consumers, or (2) control or process the data of at least 25,000 Virginia residents that also derive 50% or more of their gross revenue from the sale of personal data.

The CDPA closely follows the framework of the CCPA; however, there are a few key differences:

- The CDPA contains no private right of action. Rather, all actions must be brought by the Virginia Attorney General.

- The CDPA, like the CCPA, exempts data that is already regulated by certain listed federal laws, such as HIPAA, GLBA, FCRA, FERPA and COPPA. However, under the CDPA, the GLBA exemption is broader as it wholly exempts financial institutions, not just data subjects. Additionally, there are data-based exemptions for the Fair Credit Reporting Act, the Driver's

Privacy Protection Act, and the Federal Education Rights and Privacy Act, and nonprofit organizations.

- The CDPA contains an opt-in requirement to process sensitive personal data, unless exempted.

- The CDPA defines “consumer” more narrowly than the CCPA. The CDPA excludes those acting in a commercial or employment context.

- Under the CDPA, the “sale of personal information” requires that the consideration be monetary to qualify as a sale of data. On the contrary, the CCPA allows monetary or “other valuable consideration.”

Proposed Washington Act

The Washington Privacy Act, Senate Bill 6281 (“WPA”), is proposed legislation which mirrors the CCPA. Like the GDPR and CCPA, the WPA increases consumers’ rights with regard to their personal data and ensures businesses are transparent about collection and processing of consumer data. Additionally, the WPA enables consumers to opt out of the sale of their personal data. The WPA would apply to businesses whose products or service are targeted at Washington consumers if the business: (1) controls or processes data of more than 100,000 consumers, or (2) derives at least 50% in revenue from the sale of personal data ***and*** processes or controls personal data of more than 25,000 consumers.

The WPA and CCPA have important similarities such as: (1) a 30-day cure period; (2) business must delete a consumer’s personal data at their request; and (3) responsibility on the business to be proactive in telling the consumer what specific types of personal information the business collects and how such data is used. However, there are important differences between them:

- The WPA limits the “personal data” definition to information regarding an “identified or identifiable natural person,” whereas the CCPA definition remains broad and applies to information linked to a “particular consumer or household.”

- The WPA explicitly preempts local laws, ordinances and regulations with regard to personal data processing by controllers or processors. The CCPA does not.

- The WPA, unlike the CCPA, does not include a revenue threshold requirement.

- The WPA, unlike the CCPA, encompasses a “discrimination” provision which stops businesses from making final automated decisions.

- The WPA limits how facial recognition technology can be utilized where the CCPA has no similar provision. (The new facial recognition obligations on companies that use facial recognition would, if enacted, exceed the current obligations companies face under Washington’s Biometric Privacy Law (RCW 19.375).)

Proposed New York Act

Of all the proposed privacy legislation, the New York Privacy Act (S5642) ("NYPA") is likely the most anticipated because its language is much bolder than the CCPA. The NYPA applies broadly to "legal entities that conduct business in New York or produce products or services that are intentionally targeted to residents of New York." With such broad language, the NYPA seems tailored to reach as many businesses as possible while omitting revenue threshold language as seen in the CCPA.

Though the NYPA could change before it is enacted, its current language departs from the CCPA in two ways:

- The biggest change is that businesses would be required to act as "data fiduciaries." The proposed law states that "any entity that collects, sells or licenses personal information of consumers shall exercise the duty of care, loyalty, and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against privacy risk." This obligation would "supersede any duty owed to owners or shareholder" of an entity.

- The NYPA does not recognize implied consent. Unlike the CCPA, which does recognize implied consent, the NYPA would require businesses to demonstrate that they have obtained clear and proactive agreement from consumers where required.

Main Takeaway

The GDPR's influence in the United States is here, and it appears here to stay as more states follow suit. With two major privacy laws on each coast and variations scattered in between, it is unclear whether Congress will ultimately pass a federal law to create some uniformity. Until then, as new legislation is rolled out companies and businesses should stay up to date to protect themselves from potential regulatory action and lawsuits.

State	Regulation	Right of Access	Right of Opt-Out	Private Right of Action	Opt-in Requirement Age	Risk Assessments	Purpose or Processing Limitation
California	CCPA (eff. 1.1.2020)/CPRA (eff. 1.1.2023)	✔	✔	Only applies to violations as defined in 1798.150(a)	16	✔	✔
Virginia	CDPA (eff. 1.1.2023)	✔	✔		13	✔	✔
Washington	Washington Privacy Act, Senate Bill 6281 (Proposed)	✔	✔	✔	13	✔	✔
New York	(Proposed)	✔		✔	N/A	✔	✔

© 2024 Vedder Price

National Law Review, Volumess XI, Number 77

Source URL:https://natlawreview.com/article/gdpr-usa-new-state-legislation-making-closer-to-reality