Law360

State Privacy Law Initiatives To Prepare For In 2020

By **Amanda Lawrence, Sasha Leonhardt and David Rivera** (February 6, 2020)

Amanda Lawrence

Sasha Leonhardt

David Rivera

The California Consumer Privacy Act, which went into effect on Jan. 1, gave California residents the broadest rights in the nation to learn what data a business has about them, to request that the business delete that data and to demand that the business not sell their data.

The CCPA opened a national conversation about consumer privacy, and while the broad concept of federal privacy legislation appears to have bipartisan support in the U.S. Congress, the fact that such a law has not passed seems to have motivated other state legislatures to introduce their own consumer privacy laws.

Since the beginning of the year, at least six states have introduced new bills related to consumer privacy: Florida, New Hampshire, New York, Virginia, Washington and, once again, California, through a proposed ballot initiative. In some instances these laws mirror the CCPA and the European General Data Protection Regulation; in other ways they meaningfully deviate from these two laws.

As state legislative sessions begin and consumer privacy remains a priority for lawmakers and advocates alike, we focus on four states — New York, Washington, Virginia and California — whose proposed laws may unseat the CCPA as the nation's leading privacy statute.

New York Privacy Act

The New York Privacy Act[1] was introduced last May and continues to be debated in the current New York legislative session. If it becomes law in 2020, the NYPA may set an even higher standard for consumer privacy than the CCPA.

The NYPA would regulate the storage, use, disclosure and sale of consumer personal data by entities of any size that do business in New York or produce products or services that are intentionally targeted to its residents.

The CCPA applies only to businesses that either generate over $25 million in annual revenues; receive, sell, or share the personal information of 50,000 or more consumers; or earn at least half of their annual revenue from selling consumer data.

In contrast, the NYPA would apply to any business holding personal information about a state resident, regardless of its size. Like the CCPA, the NYPA would not apply to data collected under the federal Gramm-Leach-Bliley Act.

Other highlights of the NYPA include:

Fiduciary Duty

Going beyond the CCPA — and setting an unprecedented standard for protecting consumer

data — the NYPA would explicitly require any entity handing consumer data to "exercise the duty of care, loyalty, and confidentiality of a fiduciary." Entities holding consumer data would have to "act in the best interests of the consumer, without regard to the interests of the entity ... in a manner expected by a reasonable consumer under the circumstances." And this fiduciary duty would supersede any duty owed to owners or shareholders.

Transparency

Combining elements of both the CCPA and GDPR, the NYPA would require entities holding consumer data to disclose what data they are collecting, whether these entities are sharing or selling the data with third parties and whether the entity uses profiling — automated processing and analysis — with respect to the data that it intends to collect.

Duty to Correct

Unlike the CCPA, the NYPA provides consumers with the right to correct inaccurate or incomplete data.

Control/Opt-in

The NYPA prohibits businesses from using, processing or transferring to a third party any consumer personal data unless the consumer provides express and documented consent. The bill requires businesses to "provide consumers the opportunity to opt in or opt out of the processing of their personal data" and must do so "in such a manner that the consumer must select and clearly indicate their consent or denial of consent."

Enforcement

The NYPA would provide individuals with a private right of action for any violation of the law. In contrast, only the attorney general has unfettered rights to bring enforcement actions under the CCPA; consumers can file suit only if there was a data breach involving their unencrypted data.

Sen. Kevin Thomas — the sponsor of last year's legislation — is revising the bill based on input from industry and advocates in two hearings. Thomas has expressed optimism about prospects for passage this year, despite industry opposition.

Washington Privacy Act

Lawmakers in Washington state have reintroduced a privacy bill that would give consumers the right to control how their data is collected and used. The Washington Privacy Act[2] passed the Senate last year but fell short in the House of Representatives in the face of amendments and opposition from those seeking greater consumer privacy protections. The proposed WPA, like the NYPA, would deviate from the CCPA in a number of critical areas:

Data Protection Assessments

Companies that process personal data for targeted marketing or profiling, that process sensitive data, that process data in a way that poses a heightened risk of consumer harm or that sell personal data must conduct a data protection assessment.

This data protection assessment would need to balance the direct and indirect benefits to the company, consumers, other stakeholders and the public against the potential risks to

consumers from the new processing activity. The company must document its data protection assessment and provide a copy to the attorney general upon request. The CCPA does not require equivalent data protection assessments in these circumstances, although it does require that a company implement and maintain reasonable security procedures and practices.

Right to Correct Data

Unlike the CCPA, the proposed WPA codifies as one of its five core principles a consumer's right to "correct inaccurate personal data." However, this right is not unlimited; the WPA allows a company to take into account "the nature of the personal data and the purposes of the processing of the personal data" in offering this right to correction.

Facial Recognition

Businesses considering whether to use another company's facial-recognition technology would be allowed to independently test the technology provider's services for "accuracy and unfair performance differences across distinct subpopulations." Those subpopulations include those defined by race, skin tone, ethnicity, gender, age, disability status or other protected characteristic that is "objectively determinable or self-identified by portrayed individuals." Providers would have to address any "material unfair performance differences" that businesses identify, and businesses that use facial recognition technology in public spaces would need to provide notice, obtain consent and make information available about their facial recognition system.

Enforcement

Unlike the CCPA and the NYPA, the proposed WPA would not contain any private right of action — for data breaches, violations of the WPA or otherwise — vesting all enforcement authority with the state attorney general. It would set civil penalties as high as $2,500 for each unintentional violation and $7,500 for each intentional one. However, the WPA follows the CCPA's and NYPA's practice of exempting data that is collected, processed, sold or disclosed pursuant to the federal Gramm-Leach-Bliley Act from its coverage.

Virginia Privacy Act

The Virginia Privacy Act[3] — currently before the Virginia House of Delegates — adopts several elements from the proposed WPA that go beyond the CCPA's requirements.

The VPA, which would apply to all entities that either control the data of at least 100,000 individuals or derive more than 50% of their revenue from the sale or processing of the data of at least 25,000 individuals, would give consumers a number of rights including:

- The right to know what data is being held or processed;
- The right to correct erroneous data;
- The right to delete data; and
- The right to access their personal data.

In addition, the VPA also allows a consumer to restrict the processing of personal data if the processing is (1) not consistent with a purpose for which the data was collected; (2) not consistent with a purpose disclosed to the consumer at the time of collection or authorization; or (3) unlawful. Finally, a consumer can object to the processing of personal

data, which includes objecting for targeted advertising.

Like the bills discussed above, the VPA would exempt data that is collected, processed or sold pursuant to the Gramm-Leach-Bliley act from its coverage. Violations of the VPA would be considered violations of the Virginia Consumer Protection Act, which contain a private right of action along with enforcement by the Virginia attorney general.

California Privacy Rights and Enforcement Act

Possibly the one state that will beat all others racing to enact privacy rights stronger than those in the CCPA is ... California! Alastair Mactaggart, the real estate developer whose state ballot initiative in 2018 led legislators to quickly draft and pass the CCPA, said even before the law was effective that he was drafting a new state ballot initiative that would expand its protections.

Mactaggart's 2020 state ballot initiative, the California Privacy Rights and Enforcement Act,[4] known colloquially as CCPA 2.0, would create additional rights for consumers and obligations for companies doing business in California.

It would also create a new California Privacy Protection Agency to administer, implement and enforce the CCPA; require consumers to opt in before any sale of sensitive personal information and allow consumers to opt out of its use in advertising altogether; restrict the use of automated processing of consumer data through profiling; and expand the negligent data breach section of the CCPA, which would give consumers greater rights to pursue legal action.

Uniquely, the CCPA 2.0 initiative contains language that would allow future amendments expanding consumer rights. The initiative contains a provision that would allow any amendments that further the CCPA 2.0's purpose and intent to become law with a simple majority of the members of each House of the State Assembly and the governor's signature. To repeal any part of the CCPA 2.0, however, would require meeting the higher bar of first obtaining statewide voter approval, per the California constitution.

What Companies Can Do Now

Given the widespread legislative support in several states for enhanced privacy laws, it seems likely that at least one of the above states — and possibly more — will pass a new consumer privacy law in the coming months.

Although continued legislative debates and a changing political environment make the exact parameters of such a law unclear, there are several steps that companies can take now to prepare themselves for possible state privacy legislation:

- Track legislative developments in these four states and elsewhere to determine what new privacy legislation may require of your company;

- Monitor your company's geographic footprint to determine if you have consumers in these states who may be subject to these new laws;

- Look to the CCPA's and GDPR's standards — and the steps that others have taken to implement these laws — as guideposts for future compliance;

- Understand the data that your company currently collects, the terms under which you collect it and the permissions that consumers already may have provided regarding the use of data for analysis, marketing and sale to third parties;

- Identify how the company currently obtains consumer consent to collect personal information and revisit this as necessary to comply with new laws;

- Implement an information governance program to track, categorize and maintain control over existing and future consumer data;

- Review third-party relationships to understand how they obtain, store, use and delete consumer data;

- Evaluate your company's data security policies and procedures and ensure that they meet both legal requirements and are appropriate for your industry, data and the risks that exist to your systems and business model; and

- Ensure that your company has a data security response plan in place now, so if a data breach occurs you are well positioned to quickly protect consumer information in line with the requirements of evolving state laws.

Overall, growing commercial use of consumer data and the public's escalating concerns about it guarantee that keeping abreast of privacy and data security developments will be a challenging task. Even at this early point in the 2020 legislative cycle, several state legislatures are poised to add greater complexity and variance to the privacy and data security landscape through bills that would increase companies' substantive responsibilities when handing consumer data.

While final passage is not yet certain, all of these states — New York, Washington, California and Virginia — have active legislatures, large populations and a history of implementing strong consumer protection laws. They are key states to watch in the coming months.

Amanda Lawrence is a partner, Sasha Leonhardt is counsel and David Rivera is a regulatory

attorney at Buckley LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] S. 5642, 2019 Leg., 238 Sess. (N.Y. 2019), available at https://legislation.nysenate.gov/pdf/bills/2019/s5642.

[2] S. 6281, 66 Leg., 2020 Reg. Sess. (Wash. 2020), available at http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/6281-S.pdf?q=20200127131439.

[3] H. Del. 273, 2020 Sess. (Va. 2020), available at https://lis.virginia.gov/cgi-bin/legp604.exe?201+ful+HB473+pdf.

[4] Alastair Mactaggart, Submission of Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021 (Nov. 4, 2019), available at https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.