CONSUMER PRIVACY

HANDS OFF THE DATA

California's new data protection law gives consumers greater control over their information.

BY PAM GREENBERG

Groundbreaking. Sweeping. Influential. Those are a few of the adjectives used to describe the CCPA, the landmark data protection law set to take effect in January 2020. Formally known as the California Consumer Privacy Act, the law gives state residents the right to know what personal information businesses collect, sell or disclose about them and to opt out of the sale of that information to third parties, among many other provisions.

The law was drafted and passed very quickly in a compromise to stave off an even tougher proposed ballot initiative. It is the nation’s broadest online privacy law, affecting companies across the country that do business with California residents, and is considered a bellwether for action in other states.

In more than half the states, lawmakers introduced some kind of consumer data privacy legislation this year—a substantial increase compared with previous years. In only a few states, however, did legislation pass.

Changes Coming

The California law was enacted in June 2018 and amended later that fall, but lawmakers, consumer groups and businesses agreed that it would need further work before its effective date.

More than a dozen bills amending the act were introduced this year. At least six had passed the Legislature and were waiting for the governor to sign at press time. The changes include technical corrections, exemptions and clarifications:

• The act does not govern the collection of personal information by employers.
• “Personal information” does not include de-identified or aggregate information.
• Information lawfully available in local, state or federal government records is exempt from the law.
• Certain business-to-business transactions and communications, as well as some types of information subject to the Fair Credit Reporting Act, are exempt.
• There is a limit on the law’s private right of action so that a claim cannot be brought by those whose information was encrypted and redacted when breached.

The state also passed a new law that regulates data brokers who buy and sell personal information. It’s similar to the first-of-its-kind law Vermont enacted last year.

Other States Act

Although legislation similar to California’s was introduced in about 17 states this year, lawmakers mostly passed less controversial measures. Five states—Connecticut, Hawaii, Louisiana, North Dakota and Texas—for example, created privacy task forces, councils or studies.

On some lawmakers’ minds were the concerns of critics, including the Information Technology and Innovation Foundation, which said in a statement that, “California’s new privacy legislation will do less damage to the Internet economy than the proposed ballot initiative would have done. But even so, the bill is flawed. ... This legislation will undercut access to free content and services by prohibiting companies from penalizing consumers who opt out of sharing their personal data. This is like passing a law saying that consumers can opt out of paying for their meals, but restaurants can’t refuse them service.”

Still, a few states took measured steps forward. Nevada, like California, already had a law requiring commercial websites and online services to post a privacy policy outlining the handling of personal data. But this year state legislators went further by prohibiting those businesses from selling personal data if Nevada consumers request it not be sold.

Maine stood out this year as well. Over the past three years, many state legislatures considered, but did not pass, legislation in response to the repeal of federal internet privacy protections that would have restricted what internet service providers could do with consumer data.

Maine passed legislation that prohibits internet providers from disclosing, selling or permitting access to customers’ per-
personal information unless the customer expressly consents, with some exceptions. It also prohibits ISPs from refusing to serve a customer, charging a customer a penalty or offering a customer a discount if he or she has not opted in.

Critics say the law unfairly targets ISPs, while leaving social media and other online services to operate by less restrictive rules. Further, some say, it may be in conflict with federal law and will face legal action.

States to Watch
Washington state was widely expected to be the second to pass comprehensive consumer privacy legislation this year. The Washington Privacy Act passed overwhelmingly in the Senate early in the session, but then stalled in committee and failed to come to the House floor for a vote. It was supported by Microsoft and other tech groups, but in later versions was opposed by consumer advocates. The bill’s primary sponsor, Senator Reuven Carlyle (D), says he is committed to getting legislation passed next year.

Privacy bills in Massachusetts, New Jersey, New York and Washington were pending or had been carried over for consideration in 2020. Similar measures will likely be introduced in significant numbers again next year.

Despite calls for comprehensive federal legislation from many tech companies and from groups like the Business Roundtable, whose members are the chief executives of major U.S. companies, state lawmakers are taking the lead in protecting consumer privacy.

But the tug-of-war between those who want more restrictions and those who want fewer is far from over. California privacy activists recently signaled that they’re preparing to put an initiative on the state’s 2020 ballot that’s even tougher than the current law.

The measure would establish a data protection agency to enforce the state’s new privacy laws and would create a new class of “sensitive information”—Social Security numbers, precise location, financial data—that firms could not sell without users opting in.

Pam Greenberg follows privacy and technology-related issues for NCSL.

What Does the CCPA Do?
The California Consumer Privacy Act gives state residents the right to:
• Know what personal data is being collected about them.
• Know whether their personal data is sold or disclosed and to whom.
• Say no to the sale of personal data.
• Access their personal data.
• Request that a business delete any personal information about a consumer collected from that consumer.
• Not be discriminated against for exercising their privacy rights.

Who’s Affected?
For-profit entities that collect Californians’ personal data and meet at least one of the following:
• Annually buys, receives, sells or shares the personal information of 50,000 or more consumers, households or devices.
• Has annual gross revenue of more than $25 million.
• Derives 50% or more of its annual revenue from selling consumer personal information.

Source: Security Boulevard