Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Calif. Privacy Law To Spark GDPR-Like Compliance Efforts

By **Allison Grande**

Law360 (July 3, 2018, 10:13 PM EDT) -- The California privacy law hastily enacted last week will require online giants, telecoms, retailers and a host of others to overhaul the way they manage personal data and interact with consumers, likely prompting many companies to build on similar efforts they've made to comply with the European Union's sweeping general data protection regulation, attorneys say.

Beginning Jan. 1, 2020, companies that hold a wide range of personal data belonging to California consumers will have to comply with the stringent and unique consumer access and notice requirements contained in the California Consumer Privacy Act, which was signed into law on June 28, less than a week after being reintroduced in the state Legislature, in order to prevent a similar but potentially more stringent privacy initiative from appearing on the November election ballot.

The new California law, which gives consumers broad latitude to control how companies use and share their personal information and to request its deletion, is the first — though unlikely to be the last — of its kind in the U.S., where privacy laws are generally sector-specific and narrower. It signals the beginning of a shift among U.S. states toward more consumer-focused regimes like those in the EU, where the GDPR recently took effect and privacy is considered a fundamental human right.

With the passage of the California law, "there is an advent of a new era of consumer privacy protection that will have the force of law in the U.S.," said BakerHostetlerpartner Alan Friel. "Call it GDPR-light, or what have you, but the game has changed markedly."

While California lawmakers can and likely will make changes to the law within the next 18 months to clear up ambiguities and other disputed provisions that weren't thoroughly addressed during the rushed legislative process, "if industry thinks this maintains the status quo, they are sorely mistaken," Friel said.

Given the similarities between the California law and the GDPR — and the lack of precedence for these types of requirements in the U.S. — companies that have spent significant time over the past several years gearing up for the stringent data protection requirements of the EU law by revamping privacy policies and taking stock of the personal data they hold may find it helpful to borrow from these efforts in the scramble to get up to speed with the California law, attorneys say.

"If a company has been working toward GDPR compliance, then they've done a lot of the housekeeping that will sort of give them a head start in preparing for the California law," said Omer Tene, vice president and chief knowledge officer at the International Association of Privacy Professionals.

Under the new California law, companies will be required to tell consumers who ask what types of personal information they hold about them, what it's being used for and what third parties have access to it, and to allow consumers to opt out of the sale of their data. Consumers will also be able to request the deletion of their data, and companies will need to obtain opt-in consent before they sell data belonging to those under 16.

While some of the law's nuances are still being ironed out, attorneys don't expect lawmakers to deviate much from these basic tenets, and they recommend that companies start right away with the preliminary steps of making sure they know what data they hold on consumers and where it's located in their systems.

"In order to be able to respond to requests from users for all the types of personal data they hold on them, companies will have to know where the data is and where to pull it from, and that's an operational issue that needs to be addressed," said Tyler Newby, the co-chair of the privacy and cybersecurity practice at Fenwick & West LLP.

Those types of back-end issues are likely to be where companies see the most changes, and financial hits, in the wake of the new California law.

"For organizations in general, including law firms, they're going to have to significantly increase their budgets for information technology departments," said Laurie Fischer, managing director at HBR Consulting. "In talking to quite a few tech people and asking them what getting a whole bunch of requests to delete data would mean for their systems, they've said they would have to do at least some reprogramming, which will require more muscle and have a significant cost impact."

Everett Monroe of Hanson Bridgett LLP pointed out that many businesses have not designed their databases with consumer access to personal information in mind, and those that have have "not taken the time to create that sort of flexible database, and those that do not have a good understanding of where and how they store personal information, will find it difficult to comply with the law."

Given the similarities between the data-mapping and privacy assessment exercises required to be able to comply with consumers' enhanced rights to move and erase their data under GDPR, companies fresh off the push to get up to speed with the EU law by its May 25 implementation date could see some benefits trickle down to their efforts to comply with the new California law, attorneys say.

"If a U.S. company is required to be GDPR-compliant, the work done in terms of preparing to comply with data portability and [the] right to be forgotten will be helpful for compliance with the California statute," Pillsbury Winthrop Shaw Pittman LLP senior counsel Catherine Meyer said. "Additionally, the up-front disclosures required under the GDPR in a company’s privacy policy with respect to the categories of data being collected and the use of such data as well as the description of the new rights of consumers will be helpful."

However, attorneys were quick to note that GDPR is far from a perfect match with the California law, which is also referred to as the CCPA, making it unwise for companies that have complied with the GDPR to think there's little work left to do before 2020.

"A lot of companies that have spent substantial time and energy on GDPR compliance are going to be disappointed to learn that they can't just extend that to the California consumers and meet the requirements of the California law," said Emily Tabatabai, a member of the cybersecurity and data privacy team at Orrick Herrington & Sutcliffe LLP. "The California law is just different enough that new mechanisms and processes will be needed."

While the bills do share some similarities, including their broad definitions of personal information and their endorsement of the ability for consumers to ask companies to delete personal data that they hold, the GDPR embraces a framework that requires companies to ask users' permission before collecting any data at all, while the California law allows companies to gather data as long as they're up front in their privacy policies and other disclosures about what they're doing, but requires them to honor requests from users to opt out of the further use or sale of that data.

Because of these differences, companies will likely "need to take a fresh look at their operational compliance processes" in the coming months to ensure compliance with the California law, said Hogan Lovells partner Mark W. Brennan.

"Many companies are under the wrong assumption that GDPR compliance is sufficient, and unfortunately a number of systems that were launched by May 25 will no longer be sufficient," Brennan said.

Recognizing the differences between GDPR and the CCPA is particularly important given the breadth of companies that are expected to be swept up by the act. While the bill includes narrow exceptions for health care entities and financial service companies already covered by federal privacy laws, the IAPP in a report released Monday said the law is likely to affect more than 500,000 companies in the U.S. that collect and sell California consumers' personal information or disclose it for "business purposes."

"When these issues get talked about, people tend to think of the usual suspects, the big online platforms and maybe the data brokers," Tene said. "We released this report to show that in this case, a lot of other companies are going to be subjected to the law. It's not only going to impact California companies and Silicon Valley, but large swaths of the U.S. economy, including small and medium-sized businesses."

The broad definition of personal information, which will include types of geolocation and tracking data that is not mentioned in any other U.S. statute, will also have a significant impact on companies' compliance efforts, attorneys say.

"The definition of 'personal information' is very broad, and does not depend on identifiers like financial account numbers, date of birth or Social Security Number," said Stroock & Stroock & Lavan LLP partner Stephen J. Newman. "In other words, a business can be required to protect the privacy even of people who are not known to the business by name."

Given the sweeping nature of what constitutes personal information, a good first step for many companies to take would be to "take a close look at the broader definition of personal information under the law and think about whether they are collecting that kind of information and if they are in a position to provide the kind of disclosure that the CCPA requires," said Reece Hirsch, co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP.

These steps could also help with the enhanced liability risks that companies are likely to face under the statute, attorneys say. While the CCPA establishes a much narrower private right of action than the proposed ballot initiative would have, the new law still allows consumers to bring data breach claims after notifying the attorney general of their intentions, and to pursue damages between $100 and $750 per consumer per incident or actual damages, whichever is greater, if the attorney general decides not to pursue the claims himself.

"This could potentially be a game-changer, because until now, one of the biggest issues that consumers have had in data breach litigation is showing that there were any damages," said Robert Braun, a Jeffer Mangels Butler & Mitchell LLP partner and co-chair of the firm's cybersecurity and privacy group. "Now, with this law, they have statutory damages and just have to show that there was a breach and that their records may have been included, so I can definitely see this law making class actions a lot easier."

As the law moves closer to its 2020 effective date, attorneys say they will continue to closely track efforts by companies such as Google, Facebook, AT&T and Verizon to convince lawmakers to make changes to the law, including its enforcement mechanism and unclear definitions relating to provisions such as what it means to sell data and prohibitions on discriminating against consumers that opt out of the sale or further use of their personal data.

Those companies had at some point contributed money to a campaign to block the proposed ballot initiative, although Verizon and Facebook eventually backed down.

“It seems like the rushed CCPA was handled a bit like building a plane while trying to fly it," Brennan said. "There will need to be some technical amendments to address mislabeled sections and to clarify the intent of the drafters, including on the data disclosures and the enforcement provisions.”

Companies will also be on the lookout for any guidance put out by the California attorney general, who is expected to continue to be an active enforcer in this space, on how to facilitate consumers' opt outs and structure privacy notices, and to see whether other states follow in California's footsteps.

"I think the greatest fear that companies are facing right now is whether California will be considered the de facto nationwide law or will other states follow suit," Tabatabai said.

Given that California has long considered a leader in privacy and data security regulation — the state enacted the first breach notification law in 2003, and similar statutes are now on the books in all 50 states — "it's a very real possibility that other states may follow suit, which would present an enormous burden on businesses. It's challenging enough to comply with one state law, let alone a state-by-state matrix of similar laws," Tabatabai said.

Several other states have been especially active on privacy issues in recent years, including Illinois, New York and Massachusetts, and they are among the likely competitors for being the next to tighten the way companies use and sell their residents' data, attorneys say. The laws could even reach a more granular level, as the city of Chicago recently introduced an ordinance that would require businesses to obtain opt-in consent from city residents to use, disclose or sell their personal information; notify residents of a data breach; and register with the city if they qualify as a data broker.

"While we were kind of waiting for the government to do something" given recent incidents such as the revelation that Facebook user data ended up in the hands of political consulting firm Cambridge Analytica without users' knowledge, "states are instead jumping on this GDPR privacy bandwagon," Fischer said.

If state laws do start to spread, that may create a push for the Uniform Law Commission to set a privacy standard that all states would follow, as Braun suggested, or for the federal government to finally answer long-running calls to step in to create nationwide privacy and data security standards, according to attorneys.

"In many respects, I do think a measure like this California law does increase pressure on Washington to actually step in and advance national privacy legislation," Tene said. "This is something that we haven't seen in D.C. yet, but this law may renew pressure to act."

--Editing by Pamela Wilkinson and Kelly Duncan.