Data: Confidential

California wields a 'stick' with tough new privacy regulations. Ohio takes a 'carrot' approach.

BY RICH EHISEN

Taking a cue from the European Union's expansive new General Data Protection Regulation, California lawmakers in June adopted the toughest and most complex data privacy regulations in the United States. Given the state's history of driving national policy, the logical question is whether the California Consumer Privacy Act will inspire other states or even the federal government to impose strict new data privacy regulations of their own.

According to experts we spoke to, the answer is a definite maybe.

"Over the years several California privacy statutes have been copied by other states. But they were mostly simple and straightforward," says Kristen Mathews, a partner in the New York City law firm Proskauer Rose LLP and the head of its global privacy and cybersecurity group. "This new California law is not simple. I don't think it would be my first contender for a law that other states will copy."

She'll get no argument from David Zetoony, a partner with Bryan Cave Leighton Paisner LLP, based in St. Louis. Zetoony, head of the firm's global data privacy and security practice, calls the law "misguided, dubious in value and not well-thought-out at all."

To be sure, not everyone sees it that way. In a blog post shortly after the bill was signed on June 28, Alan Friel and Nilou Massachi, privacy attorneys for Cleveland-based Baker Hostetler LLP, called it "a win for both industry and consumers."

Meanwhile, in a statement released that same day, California Senator Bill Dodd (D), one of the measure's three authors, noted his hope that "other states will follow, ensuring privacy and safeguarding personal information in a way the federal government has so far been unwilling to do."

Senator Bill Dodd California

That remains to be seen, but Zetoony says it really doesn't matter if states follow suit or not, noting that California was the first state to adopt online privacy requirements for companies doing business there. Even though other states didn't copy them, he says most large companies adopted those policies themselves, essentially spreading the power of the law across the country.

"This law may not get emulated quickly, but it doesn't need to be to have a national impact," he says.

As noted, the California Consumer Privacy Act borrows heavily from the European Union's statute—"80 or 90 percent," Zetoony says. Whether you think that's good or bad likely depends on whether you are a consumer advocate or a big tech company that currently collects consumer data with almost unfettered access. But wherever you fall on California's privacy act, everyone agrees it is a lot less demanding than its original incarnation, which was well on its way to going before voters as a ballot initiative.

Earlier this year, a group called Californians for Consumer Privacy sponsored a drive to put a version of the state law in front of voters in November. Although it collected more than 600,000 signatures—far more than needed to get the measure on the ballot—the group said it would withdraw the proposal if lawmakers passed an acceptable privacy bill. That sparked a frenzied effort to get something through both chambers and to the governor before the June 28 cutoff date for removing the measure from

Rich Ehisen is the managing editor of State Net's Capitol Journal. This article first appeared there on Sept. 14, 2018.

the ballot. They made it with a just few hours to spare.

It's Complicated

So what exactly does that measure (AB 375) do? The short answer is a lot.

As of Jan. 1, 2020, consumers will be able to request that companies provide them with an accounting of the data they have collected on them and require the company to delete that information. Companies will have to notify consumers that they have the right to opt out of having their information sold, and businesses can't retaliate or discriminate against a consumer who chooses that option. Consumers will further be allowed to take legal action against a company that violates these or other tenets of the law.

As noted by the Harvard Business Review, the statute establishes a fairly broad definition of personal information that includes a whole raft of personal identifiers, such as geolocation, biometric data, internet browsing history, psychometric data, and inferences a company might be able to make about the consumer from that data.

There are, however, some limitations on whom the law applies to. Companies under the law must meet one of the following criteria: have annual gross revenues in excess of $25 million; process the information of 50,000 or more consumers; or derive at least 50 percent of their annual revenues from the sale of personal information.

The bill also gave the California attorney general's office the chore of drafting regulations and advising businesses about compliance with the new law. That drew the ire of Attorney General Xavier Becerra (D), who in a letter to lawmakers complained that such a mandate comprised "unworkable obligations and serious operational challenges" for his office. He also questioned the legality of the new law's civil penalties.

That led to more legislation, SB 1121, signed by Governor Jerry Brown (D), which, among several things, kills a requirement that someone suing over a data breach first notify the attorney general's office. It also delays enforcement of the law until six months after the attorney general publishes the new regulations and clarifies that consumers can file suit under the law only if the breach is caused by a company's failure to implement reasonable security steps.

That is far less than some advertising and tech companies want. The Internet Association—an industry trade group

California's Out Front in Privacy Protection

The Consumer Privacy Act is not the only example of groundbreaking consumer privacy and security legislation to come from California. The home of Silicon Valley also enacted the first law requiring companies to notify consumers of data breaches. All 50 states now have breach-notification laws like California's.

California lawmakers have passed several other privacy laws, and although only a few other states have followed suit, the Golden State's actions have had an impact beyond its borders.

Online Privacy Policies It's now common to see privacy policies posted prominently on websites and online services. That's at least partly due to California's Online Privacy Protection Act, enacted in 2003. It requires websites and other online services that collect personally identifiable information from California residents to post and comply with an online privacy policy.

The law also requires commercial websites and online services to disclose in their privacy policies how they respond to web-browser "Do Not Track" signals or similar mechanisms. Consumers can turn on these mechanisms to prevent tracking of their personal information across sites or services and over time.

An Online Eraser for Minors In another first, California passed the Privacy Rights for California Minors in the Digital World Act, known as the "Online Eraser" law, in 2013. It allows Californians under 18 to request removal of their own social media or other online postings that they later regret having shared.

It also prohibits websites or online services catering to children from advertising products or services that minors are legally prohibited from buying or are based on personal information collected about a minor.

Protecting Personal Information California law requires entities that own, license or maintain personal information to protect it. About half the states have data security laws. Some simply require that a company follow security procedures and practices; others require annual security assessments or audits, mandate training and specify that security frameworks and standards must be followed.

Assemblywoman Jacqui Irwin California

Protecting Connected Devices California recently became the first state to address security concerns surrounding the "internet of things." The new law, which passed in September with bipartisan support, requires manufacturers to equip smart devices with reasonable security features to prevent cyberattacks. Assemblywoman Jacqui Irwin (D) sponsored the bill to combat attacks that have infected routers, cameras, printers, digital video recorders and other devices. The infected devices enabled distributed denial of service attacks that shut down prominent websites and services.

"With our growing reliance on internet of things devices, the threat that unsecure devices pose to individuals, businesses and our state looms large. Ensuring we have the right tools to keep our devices and information secure is critical," Irwin says. "This new law was the result of hard work with many stakeholders from the business, technology, privacy and consumer communities."

Whether other legislatures follow its lead in these and future tech-related laws, California leaves a large footprint.

—Pam Greenberg

comprising tech giants like Amazon, Google, Microsoft, Facebook and Uber—has made clear its intention to continue working to modify the law before it goes into effect in 2020.

Several of those same companies are also lobbying the Trump administration to come up with a federal law that would override the Golden State measure.

Do Companies Have Time to Comply?

In the meantime, however, companies around the nation that do business in California are girding up to comply with the new law. Zetoony believes that how ready they are when the calendar clicks over to 2020 will be determined in great part by the effort they have already been making to comply with the European statute.

"A company that has been diligently preparing to comply with the GDPR should be in good position to comply with the California law," he says, referring to the European statute by its initials. "But if you're starting from a dead stop, I think you're going to find California's timetable very aggressive."

Mathews says that preparation is even more challenging because the ground is still shifting under the California law.

"If you really had a full year to prepare, it would be enough," she says. "But we don't really have a year because while we know there will be more amendments; we don't know what they will be. We don't want to start implementing compliance programs without knowing what the final law will look like."

Using the European statute as a model for preparation purposes is a start, but hardly a foolproof one. The law has been enforceable only since May of this year and has not yet been cited in any enforcement actions. Without that, there is no way to know if the law will hold up to legal challenges.

An Eye on Ohio

Amid so much uncertainty, Zetoony argues that states looking for a model to follow cast their eyes not to California but to Ohio, where Senators Bob Hackett (R) and Kevin Bacon (R) sponsored SB 220, aka the Ohio Data Protection Act.

That law offers Buckeye State companies that compile and transfer personal data a safe harbor from litigation over breaches if they have in place at least one of 10 specific industry-recognized cybersecurity frameworks. These are designed to "protect the security and confidentiality of personal information; protect against anticipated threats or hazards to the security or integrity of personal information; and protect against unauthorized access to and acquisition of personal information that is likely to result in a material risk of identity theft or fraud."

Ohio is the only state that uses a carrot rather than a stick regarding data privacy. Zetoony hopes it isn't the last.

"If states adopted the Ohio law," he says, "it would create a real sea change by getting far more companies to invest far more money into their data security systems."