INSURANCE JOURNAL

https://www.insurancejournal.com/news/west/2018/07/03/494203.htm

California's Data Privacy Law a Concern, Opportunity for Insurance Industry

By Don Jergler | July 3, 2018

California is on track to have what will be the nation's most far-reaching law to give consumers more control over their personal data.

The new law may be both a big concern, as well as a new and important opportunity, for the insurance industry.

Assembly Bill 375, authored by Assemblyman Ed Chau, D-Arcadia, was signed by Gov. Jerry Brown last week, hours after lawmakers passed it with no dissenting votes in a last-minute effort to convince a San Francisco real estate developer to remove a similar initiative from consideration for the November ballot ahead of a deadline.

Many saw AB 375, the California Consumer Privacy Act of 2018, as being more favorable than a voter-enacted initiative, which is more difficult to alter than laws passed through the legislative process.

The developer withdrew the initiative shortly after the law was signed.

The new law follows massive data breaches in recent years at companies like Target and Equifax, while Facebook also has faced scrutiny amid revelations that consulting firm Cambridge Analytica collected data from millions of Facebook users without their knowledge.

The law requires companies to report to customers upon their request what personal data they've collected, why it was collected and what third-parties have received it.

The law doesn't take effect until Jan. 1, 2020, but it's already gotten the attention of people who are warning of potential liabilities for companies that don't take the time to understand the law, or decide not to obey it.

This law is similar to Europe's General Data Protection Regulation. GDPR data privacy regulations took effect in May. Those regulations also aim to give consumers greater control over use of their data.

GDPR overhauls data protection laws in the European Union, and foresees fines of up to 4 percent of global revenues for companies that break the rules. GDPR forces companies to implement data storage, processing and marketing best practices, and enables consumers to request to be forgotten – meaning companies must remove all their data.

"The California privacy bill is a natural progression of GDPR," said Jeff Brown, vice president of Imprezzio, a technology software company that serves the insurance industry. "We believe this measure was accelerated by (Facebook founder and CEO Mark) Zuckerberg's Congressional testimony on the use of consumers data and the strong desire by consumers to understand and control their data – it is a social rights issue."

Joan D'Ambrosio, a partner in San Francisco-based law firm Clyde & Co., who focuses on technology, media and privacy for insurers, is urging the insurance sector to watch this new law closely.

“From an insurance perspective it certainly creates the potential for more liability for companies and therefore for their insurers,” D’Ambrosio said. “There’s no question it will create potential liability.”

The new California law provides for its enforcement by the state attorney general, and provides a private right of action “in connection with certain unauthorized access and exfiltration, theft, or disclosure of a consumer’s nonencrypted or nonredacted personal information.”

It also creates a Consumer Privacy Fund with in the state’s General Fund to be used to support the purposes of the bill and its enforcement.

Companies that violate the law could not only face penalties, but lawsuits as well, D’Ambrosio said.

“The potential exposure would be down the line if companies deviate from the requirements,” she added.

The new law lays out numerous consumer rights, including that consumers will have the right to request that a business that collects personal information about them must disclose to the consumer the following:

- The categories of personal information it has collected about that consumer.
- The categories of sources from which the personal information is collected.
- The business or commercial purpose for collecting or selling personal information.
- The categories of third parties with whom the business shares personal information.
- The specific pieces of personal information it has collected about that consumer.

The law also requires a business that collects personal information about consumers to disclose the categories of personal information it has collected about them, the categories of sources from which the personal information is collected, the purpose for collecting or selling personal

information, the categories of third parties with which the business shares personal information and the specific pieces of personal information the business has collected about that consumer.

D'Ambrosio believes the law will undergo further modifications as the state works out how to enact and enforce it.

"A lot of the details now are to be fleshed out," she said. "But there is going to be a much higher level of accountability about the collection and usage of the information."

The law also creates an opportunity for the insurance industry to sell more cyber policies, said Joshua Motta, CEO of Coalition, who was quick to point out that there are key differences between the new California law and GDPR.

"Under GDPR fines and penalties are not insurable," he said, noting that in most EU states, only defense costs are insurable under the regulation. "With California, all of the fines and penalties are insurable."

He added, "It's a significant tailwind to purchase the insurance."

San Francisco, Calif.-based Coalition was co-founded by Motta and fellow technology entrepreneur John Hering. Licensed as an insurance producer, the managing general agent offers customers free cybersecurity tools, and business customers can acquire up to $10 million of insurance coverage.

Motta said the firm fielded numerous calls from brokers after GDPR went into effect, and he expects more of the same following the new California law.

The law calls for fines of up to $7,500 per record loss, which will serve as a loud wakeup call for businesses without cyber liability coverage.

"Companies aggregating data, they now have just a massive, massive loss exposure if that data is breached," Motta said. "That is an unforeseen business expense that can be catastrophic, it can be company ending. It's getting to the point where businesses cannot afford to be uninsured."

The law covers a broad array of companies. It includes any for-profit company doing business in California that has revenues greater than $25 million, that receives more than 50,000 unique personal records per year or that derives more than 50 percent of its annual revenue from selling personal information.

Motta noted that something as simple as the IP addresses of a website's visitors from California may be considered personal information.

"If you have 50,000 or more IP addresses, then you are subject this new law," he said. "This has a very wide-ranging impact on businesses across the country."

Brown is advising companies that collect data in California or in Europe to consider creating a new position, which he calls a data protection officer, to help companies deal with the new law.

"Make sure this person has the expertise you need," Brown advised. "They can help you redesign what consent and disclosure looks like for your customers. Consumers will need to check a box (or its equivalent) for every single use-case you have for their data. They need to be able to select those they agree with and decline those they don't, and you need to be able to comply and track their preferences in your systems.

He also advises that companies consider what third-party providers are doing as well.

"Remember, if a third-party is not able to prove their GDPR compliance, the work they do for your EU data is illegal," he said. "Audit your third-party providers and re-evaluate service level agreements."

California's position as the nation's most populous state already makes the new law of nationwide interest, however D'Ambrosio expects other states to follow California's lead with data privacy.

"There are a lot of people who are drawing analogies with GDPR with this particular act that it's likely to cause a cascade of legislation around the country trying to meet privacy standards," she said. "It's very likely that these standards will continue to change."

Related:

- Far-Reaching Data Privacy Bill Approved in California
- GDPR Day 1: Privacy Activist Files Complaints Against Tech Giants Over 'Forced Consent'
- GDPR Day 1: Wake-Up Call for Many; Media Sites Shut EU Access