Countdown to California's New Privacy Act

by **STACEY GARRETT** — September 26, 2019 *in* **Data Privacy**, **Featured**

Keesal, Young & Logan's Stacey Garrett does a deep dive into how organizations can be preparing for the California Consumer Privacy Act (CCPA), going into effect on January 1, 2020.

In June 2018, California broke new ground when it was the first state in the nation to enact a comprehensive data privacy law. The new law, called the California Consumer Privacy Act, was fueled by a national debate over who owns an individual's personal information: the

individual, or the business that collected it. California lawmakers answered that question by giving consumers significant new rights to control their personal information and by requiring that businesses covered by the CCPA be transparent about how they collect, use and share that information. The CCPA takes effect on January 1, 2020. Experts estimate that the CCPA will apply to more than 500,000 businesses in the United States.

"Personal Information" Covered by the CCPA

The CCPA has one of the most expansive definitions of "personal information" on the planet. It includes not only the traditional categories of personal information (such as an individual's name, social security number and driver's license number), but it also includes more unusual categories such as a person's internet protocol (IP) address, alias, geolocation data, professional or employment-related information, browsing and search history, purchasing history and all inferences drawn from that information. And that is just a partial list.

New Rights for Consumers

Starting on January 1, 2020, California consumers (essentially anyone who is a resident of California) will have new rights over the personal information that is collected by businesses subject to the CCPA. These rights include:

- **Rights of Disclosure and Access** – Consumers will have the right to request that businesses disclose what personal information the business has collected about the consumer, how it is used and whether the information has been sold or shared with third parties. Consumers also will have the right to access the personal information that has been collected about them. Businesses must provide the information free of charge and in a readily useable format within 45 days of receiving a verifiable consumer request.
- **Right to Deletion** – Consumers will have the right to request that businesses delete personal information that has been collected from the consumer. Unless a recognized exception applies (and there are nine), the business must delete the personal information from its records.
- **Right to Opt-Out** – In certain circumstances, consumers will have the right to opt-out of having their personal information shared or sold. Businesses must respect a consumer's decision to opt-out for 12 months.
- **Right to Nondiscrimination** – Consumers will have the right not to be treated differently simply because they have exercised their rights under the CCPA. Businesses can, however, offer consumers incentives to share their personal information.

New Obligations for Businesses

The CCPA also imposes specific obligations on covered businesses. Businesses will need to:

- Revise their privacy notices to disclose information about their information collection and sharing practices and to inform consumers of their rights under the CCPA.
- Revise and update their vendor and service provider processing agreements to make it clear that vendors and service providers are prohibited from selling, retaining, using or

disclosing the consumers' personal information for any purpose other than providing the services provided by the contract.

- Make available to consumers two or more designated methods for submitting requests for information the business has collected and sold about the consumer including, at a minimum, a toll-free telephone number and a website address, if the business maintains a website.
- If the business sells consumers' personal information, provide a clear and conspicuous link on the business's internet homepage titled "Do Not Sell My Personal Information" that links to an internet webpage that enables the consumer to opt-out of the sale of the consumer's personal information.
- Educate and train employees who are responsible for handling consumer inquiries about the business's privacy practices so the employees can direct consumers on how to exercise their rights under the CCPA.

Solutions on the Horizon

The CCPA likely is just the beginning of a broader movement to give individuals greater control over their personal information and to require that businesses be transparent about their collection and use of that information. In the year since California enacted the CCPA, 13 states have followed in California's footsteps by introducing similar comprehensive data privacy bills, and another six states are considering additional privacy regulations.

Although federal lawmakers may eventually create national uniformity by enacting a comprehensive federal data privacy law, so far those efforts have not gotten much traction. Consequently, businesses that conduct business in California and elsewhere will have to decide whether they plan to roll out a state-by-state privacy strategy or whether they will adopt a comprehensive program that provides broad rights for all individuals, despite their state of residence.

Regardless of which strategy businesses choose, businesses will want to develop processes that comply with applicable laws while simultaneously minimizing the time and expense burdens associated with manually responding to consumer requests. To ensure timely, efficient and consistent compliance, companies will benefit by streamlining and automating their responses to consumer inquiries by using workflow automation software. In addition to tracking consumer requests and accelerating company response time, workflow automation also creates a verifiable audit trail that allows businesses to document their compliance for regulatory and corporate governance purposes.

Tags: CCPA/California Consumer Privacy Act

Previous Post

Why Hong Kong is China's Sanctions Hot Spot

Stacey Garrett

Stacey Garrett is a shareholder of Keesal, Young & Logan and is located in Long Beach, California. Stacey is certified by the International Association of Privacy Professionals (IAPP) in the areas of United States and European Union privacy law and also holds certifications in privacy management and technology. Stacey graduated magna cum laude from the University of California, Hastings College of Law and is a member of the Order of the Coif. Stacey is admitted to practice law in California, Nevada and before the Supreme Court of the United States. You can connect with Stacey on LinkedIn.

Related Posts

Why Hong Kong is China's Sanctions Hot Spot

September 25, 2019

What Factors Influence a Company's Ethical Culture?

September 25, 2019

Chief Compliance Officers Need Real-Time Technology Just to Keep Up These Days

September 25, 2019

On ADA Website Compliance, the DOJ Has a Chance to End the Chaos in the Courts

September 24, 2019

Type your email

Subscribe to the Newsletter

☐ In addition to the newsletter, I understand I may also receive occasional information about webinars, events or GRC resources. I can unsubscribe from the newsletter or special offers at any time. Privacy policy available at link in footer.

Submit

SEC Litigation News

Andres Fernandez and Edison Denizard SEPTEMBER 25, 2019

SEC Charges Principals of Music Entertainment Company with Multi-Million Dollar Offering Frauds and Ponzi Schemes

David R. Gibson, et al. SEPTEMBER 25, 2019

SEC Obtains Final Judgment Against Former Officers of Wilmington Trust

James Alex Irvin SEPTEMBER 25, 2019

SEC Charges PetMed Express Former Executive with Repeated Insider Trading

Jump to a Topic:

anti-corruption anti-money laundering/AML Artificial Intelligence/A.I. automation banks Big Data blockchain board of directors board risk oversight bribery business ethics leadership leadership alliance CCPA/California Consumer Privacy Act cloud computing communications management corporate culture corporate governance culture of ethics cyber risk data analytics data breach data governance decision-making Dodd-Frank DOJ due diligence ethics and compliance fcpa enforcement actions GDPR GRC HIPAA information security internal audit internet of things KYC/know your customer machine learning mergers and acquisitions monitoring reputational harm risk assessment risk management SEC third party risk management tone at the top training whistleblowing