NEWMEYER & DILLION LLP

CALIFORNIA'S BOLD NEW DATA PRIVACY LAW: WHAT YOU NEED TO KNOW TO COMPLY

By: Anne J. Kelley

Anne J. Kelley

Contact

925.988.3223
Anne.Kelley@ndlf.com

Practice Areas

Construction Litigation
Cybersecurity
Insurance Law

2018 has been a pivotal year for consumer data protection, with sweeping new laws being passed to ensure increased consumer data privacy around the world. In May, Europe's General Data Protection Law, or GDPR, took effect. In June, the California Legislature passed the California Consumer Privacy Act of 2018 ("CCPA"), a bold new digital data privacy law that is the first of its kind in the United States. The California law becomes effective on January 1, 2020, and will launch a new era of data privacy and protection in the U.S. The new law will force significant changes on companies that collect and sell personal data and will provide consumers with greater protection and control over their personal data.

The Growing Need Behind the CCPA

The impetus behind the California law was recent data sharing and privacy scandals. In March, Facebook admitted that it passed data on as many as 87 million users to third parties, including to British political consulting firm Cambridge Analytical. Facebook also admitted entering into data-sharing partnerships over the last decade with at least 60 device-makers, giving them access to users' data. These agreements included Chinese company Huawei, which U.S. intelligence officials view as a national security threat. Because of these scandals and recent, large data breaches, consumers are becoming more and more concerned about privacy, the exposure of their personal information, and companies' seemingly unfettered data sharing practices.

Consumers' Rights Under the CCPA

The new California law provides consumers with certain basic rights when it comes to their personal information:

1. The right to ask a business to disclose the categories and specific pieces of personal information the business has collected.
2. The right to have a business delete any personal information it has collected.
3. The right to know what personal information a business has collected about them, where the data was sourced from, what it is being used for, whether it is being sold or disclosed and to whom it is being sold or disclosed.
4. The right to opt out of allowing a business to sell or disclose their personal information to third parties for a business purpose.
5. The right to receive equal service and pricing from a business, even if exercising privacy rights under the law.

Does the CCPA Apply to My Business?

The California law will apply to for-profit businesses that collect and control California residents' personal information, do business in the State of California and meet any of the following criteria:

1. Have annual gross revenues in excess of $25 million; *or*
2. Receive or disclose personal information of 50,000 or more California residents, households or devices on an annual basis; *or*
3. Derive 50% or more of their annual revenue from selling California residents' personal information.

The law is broad enough to include not only large companies that have an on-line presence and brick-and-mortar stores, but many smaller businesses as well, even if they are not physically present in California. After all, companies that deal in consumer data typically will have some California customers.

Here's What You Need to Get Ready: Data Collection, Disclosures, and Best Practices

By January of 2020, businesses will need to have methods in place to monitor their data collecting and data sharing practices and the resources in place to provide requested information to consumers quickly. Among other things, companies required to comply with the CCPA will need to:

1. Determine what personal data they are collecting from individuals and for what purposes, where the data comes from, whether it is being sold or disclosed, and to whom.
2. Provide at least two methods for consumers to submit requests for disclosure, including, at a minimum, a toll-free telephone number and a Web site address.
3. Disclose requested information free of charge to the consumer within 45 days of receiving the request, subject to certain extensions.
4. Disclose if they sell consumer data to third parties and give consumers the ability to opt out of the sale by placing a link entitled "Do Not Sell My Personal Information" on their Web site's home page.
5. Update their privacy policies prior to January 1, 2020 and every 12 months thereafter to make the disclosures the law requires.
6. Refrain from selling personal information of a consumer younger than 16 without that consumer's affirmative consent (or, if younger than 13, the consent of their parents).

The CCPA also requires that companies take more precautions to protect the personal data they collect in an effort to prevent the exposure of personal information from data breaches. The law requires that companies "implement and maintain reasonable security procedures and practices" to ensure that consumers' private information is not exposed in a security breach. What constitutes "reasonable security procedures and practices" is not set forth in the law. Individuals or the state attorney general may bring lawsuits if consumers' personal information is exposed due to a breach of the duty to implement reasonable security procedures and practices.

Potential Changes on the Horizon

Because the CCPA was passed very quickly by the California Legislature and is expected to have such a broad impact, the Legislature left open the possibility of amendments to the law. We expect that amendments will take place and that the state attorney general will develop compliance guidelines in the upcoming months.

In an age of ever-expanding internet use, security breaches, and increasing questions about data collection and sharing, the California Consumer Privacy Act of 2018 may just be the tip of the iceberg when it comes to regulating digital data, privacy of personal information and the collection and use of individuals' personal data.

Anne Kelley is a partner in Newmeyer & Dillion's Walnut Creek office where she passionately advises businesses in the areas of cybersecurity, cyber insurance and data privacy issues, including compliance with the recent GDPR and California Consumer Privacy Act of 2018. With over three decades of experience advising policyholders on complex insurance coverage matters and litigating coverage matters in state and federal court, she brings that experience to the arena of cyber insurance coverage. Anne works to educate companies on cybersecurity and data privacy issues and assists companies to obtain cyber insurance coverage tailored to respond to their specific cyber risks. For more information on how Anne can help, please contact her at anne.kelley@ndlf.com.

ABOUT NEWMEYER & DILLION LLP

For more than 30 years, Newmeyer & Dillion has delivered creative and outstanding legal solutions and trial results for a wide array of clients. With over 70 attorneys practicing in all aspects of business, employment, real estate, construction and insurance law, Newmeyer & Dillion delivers legal services tailored to meet each client's needs. Headquartered in Newport Beach, California, with offices in Walnut Creek, California and Las Vegas, Nevada, Newmeyer & Dillion attorneys are recognized by The Best Lawyers in America©, and Super Lawyers as top tier and some of the best lawyers in California, and have been given Martindale-Hubbell Peer Review's AV Preeminent® highest rating.

For additional information, call 949.854.7000 or visit www.ndlf.com.