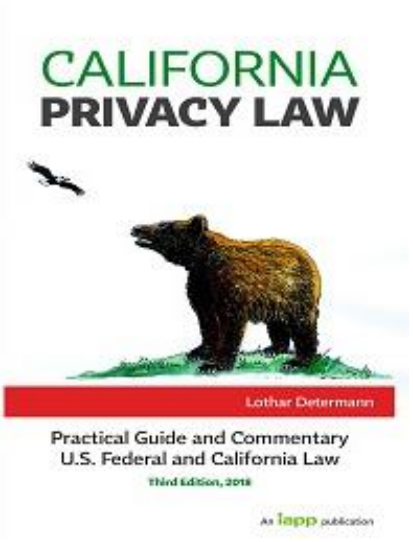
iapp

Lothar Determann

Broad data and business regulation, applicable worldwide

As of January 1, 2020, companies around the world will have to comply with additional regulations related to processing of personal data of California residents. Pursuant to the California Consumer Privacy Act of 2018, companies have to observe restrictions on data monetization business models, accommodate rights to access, deletion, and porting of personal data, update their privacy policies and brace for additional penalties and liquidated damages.



Available in print and ebook

The California Legislature adopted and the governor signed the bill on June 28, 2018, after an unusually rushed process in exchange for the proposed initiative measure No. 17-0039 regarding the Consumer Right to Privacy Act of 2018, also known as the "ballot initiative," being withdrawn from the ballot the same day, the deadline for such withdrawals prior to the November 6, 2018 election.

In total, the California Consumer Privacy Act adds to the California Civil Code about 10,000 new words and Sections 1798.100 to 1798.198. In recitals, the legislature acknowledges some of the many existing data privacy laws that California has already enacted over the years. California has led the United States and often the world in codifying privacy protections, enacting the first laws requiring notifications of data security breaches (2002) and website privacy polices (2004). In the operative section of the new law, however, the California Consumer Privacy Act's drafters did not address any overlap or inconsistencies between the new law and any of California's existing privacy laws, perhaps due to the rushed legislative process, perhaps due to limitations on the ability to negotiate with the proponents of the Initiative. Instead, the new Cal. Civ. Code §1798.175 prescribes that in case of any conflicts with California laws, the law that affords the greatest privacy protections shall control. Notably Cal. Civ. Code §1798.194 instructs courts that the new law "shall be liberally construed to effectuate its purposes."

Consequently, companies, privacy officers, lawyers and others will have to deal with an even more complex and fragmented privacy law landscape in California, and therefore in the United States and the world. Given the impact of California on the global economy as the 5th largest, behind only the United States as a whole, China, Japan and Germany, most global companies will have to continue to do business in California.

This initial overview answers four key practical questions that my California Privacy Law guide and commentary already covers with respect to California's other privacy laws. It then offers some basic comparisons to the ballot initiative and the EU General Data Protection Regulation, and concludes with my outlook. I welcome your thoughts, questions and comments and look forward to additional views and insights.

Who and what data is protected?

Principally, all California residents are protected under the California Consumer Privacy Act with respect to any information that relates to them.

Californians are not just protected in their roles as consumers, but also as employees, patients, tenants, students, parents, children, etc. Cal. Civ. Code §1798.140(g) defines "consumer" as any "natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier. "According to these regulations, a "resident" "includes (1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose," subject to a number of clarifications and specifications set forth in Section 17014 of Title 18 of the California Code of Regulations.

Unlike other sections of the California Civil Code, however, or any other privacy laws, Cal. Civ. Code §1798.140(o)(1) defines the term "personal information" broadly as "any information that ... relates to ... a particular consumer or household." Data can be protected even if it does not relate to a single individual (since "households" are covered) and if it does not contain a name. For example, annual water or energy consumption of a household, a particular employee's job description, an Internet Protocol address, web browsing history and "purchasing tendencies" will be regulated as personal information, even if no names are associated with it.

A number of limited and complex exceptions apply to this definition. For example "publicly available information" (Cal. Civ. Code §1798.140(o)(2)) and "commercial conduct [that] takes place wholly outside of California" (Cal. Civ. Code §1798.145(a)(6)) are excluded.

Who must comply?

Companies around the world have to comply with the California Consumer Privacy Act if they receive personal data from California residents and if they— or their parent company or a subsidiary— exceed one of three thresholds: (a) annual gross revenues of $25 million; (b) obtains personal information of 50,000 or more California residents, households or devices annually; or (c) 50 percent or more annual revenue from selling California residents' personal information. Parent companies and subsidiaries using the same branding are covered in the definition of "business," even if they themselves do not exceed the applicable thresholds.

(a) Companies must comply if they have annual revenues in excess of U.S. $25 million. It is not clear whether this number needs to include only their California revenue or global sales. While Cal. Civ. Code § 1714.43(a)(1) defines the scope of the California Transparency in Supply Chains Act expressly in reference to "annual worldwide gross receipts," the new Cal. Civ. Code §1798.140(c)(1)(A) merely refers to "annual gross revenues" without an expanding reference to "worldwide." Yet, a limiting reference to California is also missing, as for example contained in Section 17942(a)(2) of the California Revenue and Taxation Code, which refers to "total income from all sources derived from or attributable to this state."

(b) A company would need to comply if it obtains personal information of at least 50,000 California residents annually. Companies may pass this threshold more quickly than anticipated because the scope of personal information is broad. Most companies operate websites and inevitably capture IP addresses. Notably, companies need to comply regardless of whether the website targeted businesses or individual customers in California given that the term "consumer" is defined to mean any "resident." Even individual bloggers and relatively small businesses outside California may find it difficult to ensure that they do not receive personal information of more than 50,000 California resident visitors to their website annually, simply from having it be passively accessible from there, and, within California, most retailers, fitness studios, music venues and other businesses will meet this threshold.

(c) Companies can also be subject to the law based on whether they sell California residents' personal information. A relatively small company in California may need to comply if it derives more than 50 percent of its annual revenue from selling California residents' personal information. "Selling" is defined broadly to mean any disclosing or making available for monetary or other valuable consideration, subject to a number of exceptions set forth in Cal. Civ. Code §1798.140(t), including consumer-directed disclosures to third parties that do not sell the personal information, limited sharing with service providers, and business transfers in bankruptcy, M&A and similar transactions.

(d) A company without a physical presence or affiliate in California may be able to avoid complying with the statute, however, if it can ensure that its "commercial conduct takes place wholly outside of California" for purposes of Cal. Civ. Code §1798.145(a)(6)) and that it is not doing "business in the State of California" for purposes of Cal. Civ. Code §1798.140(c)(1). Most U.S. companies will find it difficult to determine that they are not doing business in the state of California, because the term "doing business" is generally understood very broadly. According to California Revenue and Taxation Code Section 23101(a) an out-of-state company is "doing business in California if it actively engages in any transaction for the purpose of financial or pecuniary gain or profit in California." Furthermore, according to California Corporations Code Sections 191(a), 15901.02(ai) and 17708.03(a), companies outside of California and qualified to do business in California may be subject to the law if they enter "into repeated and successive transactions" in California, which could occur remotely and online.

How to comply?

Companies will need to take a number of affirmative steps to comply with the new requirements, including the following:

- **Prepare data maps, inventories or other records** of all personal information pertaining to California residents, households and devices, as well as information sources, storage locations, usage and recipients, to add newly required disclosures to privacy policies, to prepare for data access, deletion, and portability requests, to secure prior consent for data sharing from parents and minors and to comply with opt-out requests to data sharing.
- **Consider alternative business models and web/mobile presences**, including California-only sites and offerings, as suggested in Cal. Civ. Code §1798.135(b) and charges for formerly free services to address the complex and seemingly self-contradictory restrictions set forth in Cal. Civ. Code §1798.125 on a company's ability to impose service charges on California residents who object to alternate forms of data monetization.
- **Make available designated methods for submitting data access requests**, including, at a minimum, a toll-free telephone number, pursuant to Cal. Civ. Code §1798.130(a).
- **Provide a clear and conspicuous "Do Not Sell My Personal Information" link** on the business' Internet homepage, that will direct users to a web page enabling them, or someone they authorize, to opt out of the sale of the resident's personal information, per Cal. Civ. Code §1798.135(a)(1).
- **Fund and implement new systems and processes** to comply with the new requirements, including to:
    - Verify the identity and authorization of persons who make requests for data access, deletion or portability.
    - Respond to requests for data access, deletion and portability within 45 days.
    - Avoid requesting opt-in consent for 12 months after a California resident opts out, per Cal. Civ. Code §1798.135(a)(5).
- **Update privacy policies** with newly required information, including a description of California residents' rights per Cal. Civ. Code §1798.135(a)(2).
- **Determine the age of California residents** to avoid charges that the company "willfully disregards the California resident's age" and implement processes to obtain parental or guardian consent for minors under 13 years and the affirmative consent of minors between 13 and 16 years to data sharing for purposes of Cal. Civ. Code §1798.120(d); companies can try to obtain parental consent by providing a consent form to be signed by the parent and returned via U.S. mail, fax, or electronic scan.

What sanctions and remedies do companies face?

According to the new Cal. Civ. Code §1798.155, companies can be ordered in a civil action brought by the California Attorney General's Office to pay penalties of up to $7,500 per intentional violation of any provision of the California Consumer Privacy Act, or, for unintentional violations, if the company fails to cure the unintentional violation within 30 days of notice, $2,500 per violation under Section 17206 of the California Business and Professions Code. Twenty percent of such penalties collected by the State of California shall be allocated to a new "Consumer Privacy Fund" to fund enforcement.

According to the new Cal. Civ. Code §1798.150, companies that become victims of data theft or other data security breaches can be ordered in civil class action lawsuits to pay statutory damages between $100 to $750 per California resident and incident, or actual damages, whichever is greater, and any other relief a court deems proper, subject to an option of the California Attorney General's Office to prosecute the company instead of allowing civil suits to be brought against it.

Companies, activists, associations and others can be authorized to exercise opt-out rights on behalf of California residents according to Cal. Civ. Code §1798.135(c).

California Consumer Privacy Act and the initiative compared

The California Consumer Privacy Act implements many principles originally contained in the ballot initiative, but it notably moves the effective date from August 2019 to January 1, 2020. The California legislature can modify the California Consumer Privacy Act by simple legislative majority, whereas the initiative would have required another voter ballot or a 70 percent legislative majority and only allowed modifications that "are consistent with and further the intent of this Act." Also, the California Consumer Privacy Act scales back the options and incentives for enforcement through private litigation and provides greater differentiation in its restrictions regarding offers of charge-free and for-charge versions of services, depending on whether consumers opt out of or into data sharing (whereas the initiative contained an absolute prohibition of charges for consumers who opt out of data sharing). On the other hand, the California Consumer Privacy Act lowered the "big company threshold" to $25 million annual revenue whereas the Initiative had contemplated a $50 million threshold. Sponsors of the initiative published additional comparison points here.

California Consumer Privacy Act and EU GDPR compared

Companies around the world have been working feverishly on taking steps to comply with the EU General Data Protection Regulation, the first significant update of data protection laws in Europe for more than 20 years. The GDPR took effect on May 25, 2018, and required significant changes to documentation and data handling practices.

Some companies implemented many of their new privacy protection measures worldwide in the hopes of being able to avoid having to make further jurisdiction-specific updates for a while. The passage of the California Consumer Privacy Act has now raised the question as to whether these measures will be sufficient to the extent they reach California residents with their GDPR-related compliance measures. Unfortunately, the answer is largely, "No."

Global companies can and should try to address the requirements of the California Consumer Privacy Act, EU GDPR and other privacy regimes simultaneously and holistically in the interest of efficiency. But companies cannot just expand the coverage of their EU GDPR compliance measures to residents of California. For example, the California Consumer Privacy Act:

- Prescribes disclosures, communication channels (including toll-free phone numbers) and other concrete measures that are not required to comply with the EU GDPR.
- Contains a broader definition of "personal data" and also covers information pertaining to households and devices.
- Establishes broad rights for California residents to direct deletion of data, with differing exceptions than those available under GDPR.
- Establishes broad rights to access personal data without certain exceptions available under GDPR (e.g., disclosures that would implicate the privacy interests of third parties).

- Imposes more rigid restrictions on data sharing for commercial purposes.

The EU GDPR leaves companies with the discretion to offer consumers a choice between for-charge services and charge-free services conditioned on informed, voluntary, specific and express consent to data monetization. Under Cal. Civ. Code §1798.125(a)(1), on the other hand, a "business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights ... including ... by ... charging different prices or rates ... including through the use of discounts or other benefits. ..." Under the California regime, if companies want to continue offering a charge-free service to Californians, companies cannot rely on revenue from data sharing or other usage to fund the service, because Californians can opt out of data sharing and demand data deletion. According to Cal. Civ. Code §1798.125(b)(3), companies may offer financial incentives to California residents, including compensation, for the collection or sale of their personal information, but only if they obtain prior opt-in consent which may be revoked by the customer at any time.

Outlook

Companies around the world will need to start working right away to assess the California Consumer Privacy Act's impact on their business, systems and data handling practices. A year and a half is not a lot of time as anyone who has been working on EU GDPR compliance knows well.

The California legislature should also start working right away— on repealing, or at minimum simplifying and aligning the provisions within the California Consumer Privacy Act, as well as the dozens of existing privacy laws that are now partially or fully obsolete and create unnecessary complexities for companies within and outside California, particularly now that California has moved from sector- and harm-specific privacy legislation to a much broader and comprehensive privacy regime with the California Consumer Privacy Act. To keep its leadership role in privacy protections, the California legislature also has to play its part in keeping privacy protections and doing business in California manageable.

At the same time, Congress should consider whether it is time for a federal privacy law that harmonizes or preempts the fragmented landscape of divergent state privacy laws, including the 49 different state laws on data breach notifications that followed California's 2002 law and make it unnecessarily difficult and costly for companies to deal with crisis situations when they become victims of cyber attacks and data theft. The U.S. deliberately decided against overbroad federal data regulations from the 1970s until recently, and many good reasons against preemption still exist. However, California Consumer Privacy Act may drive the fragmentation of state law to the level that consensus may coalesce around suitable federal regulation.

Last but not least, all of us in California and elsewhere should carefully consider and apprise our government representatives of how much we value free services versus data regulation. A day before the California Consumer Privacy Act was enacted, Eric Goldman analyzed its potential impact and raised the crucial question whether consumers are getting a good deal. We have been told for decades that there is no privacy online. Yet, we have embraced many innovative services, which would probably never have gained critical mass or developed if companies had to rely on consumer fees for the initial launch. Highly publicized and litigated privacy intrusions have neither stopped nor slowed down the rapid expansion of charge-free email, online news, maps, mobile apps or social media.

Someone will have to pay somehow for the additional compliance efforts required by the California Consumer Privacy Act, including toll-free numbers, privacy notices, opt-in and opt-out mechanisms, data access, data deletion, and data portability, as well as for lost revenue from now prohibited data monetization models and the costs of prosecution, litigation, penalties and statutory damages that businesses will have to pay when they become victims of cyber attacks or data theft even where no one suffers any actual damages. Larger companies may be able to absorb some of the costs or apply expenses to a broader geographic customer base (i.e., consumers

in other states or countries). Small businesses in California have far less options. At the end of the day, we as consumers will bear the costs.

Opinions expressed in this article are those of the author, and not of his firm, clients or others. The author is grateful for valuable input from Catherine R. Gellis, Mariam Abdel-Malek and his Baker McKenzie colleagues Danielle Benecke, Brian Hengesbaugh and Andrea Tovar.

Illustration: Lothar Determann, used with permission.

Author

Lothar Determann