CCPA 100-Day Compliance Checklist: It's Not Just About the Privacy Policy

September 2019

Authors: **Steven R. Chabinsky, F. Paul Pittman**

With only 100 days left in 2019 as of the date of this publication, the California Consumer Privacy Act (CCPA) will be here before you know it. As we have described previously, the CCPA applies to a wide range of for-profit companies (and potentially their subsidiaries) that do business in California.

By way of example, the CCPA may cover retail businesses that process consumer personal information both online and in physical stores. It may cover social media companies that collect usage and geolocation data through apps, as well as the advertising and marketing entities that collect and share data on consumers behind the scenes for use in creating profiles and serving ads. Data brokers whose business models are built on buying and selling personal information will be especially impacted by the CCPA. Even banks and other financial service businesses that collect the personal information of California residents, when unrelated to their purchase or offering of certain financial products or services (as defined under the GLBA), may be subject to the CCPA.

Among other things, the CCPA requires businesses to be transparent about their practices relating to the collection, sale and disclosure of personal information from California residents, in both their public disclosures and in responding to consumer requests. Businesses that do not comply with the CCPA face statutory penalties. The California Attorney General (Cal AG) can seek injunctive relief and penalties of up to US$2,500 for each violation or US$7,500 for each *intentional* violation of the CCPA. While it is true the Cal AG cannot bring enforcement actions until July 2020, it remains unclear whether those actions can take into account CCPA violations that existed as of the January 1, 2020 effective date. Perhaps more threatening is that, in addition to Cal AG enforcement, the CCPA provides consumers with a private right of action to seek pecuniary or statutory damages ranging from US$100 to US$750 per consumer, per incident, as a result of a data breach caused by a business' lack of reasonable security. There is no six-month delay when it comes to individual and class actions.

Yet, despite the fact that the CCPA compliance deadline has been looming for over a year now, many companies remain unprepared. Fortunately, businesses that have yet to begin their CCPA compliance efforts can still achieve compliance in a timely manner. Efforts, however, must begin now. For starters, and as further outlined below, businesses must recognize that compliance requires more than simply revising their online privacy policy. Similar to the GDPR, the foundation of the CCPA is built on individual rights that extend well beyond a company providing sufficient notice to the public of its privacy practices.

CCPA Compliance Checklist

Although the final regulations have yet to be promulgated, the general requirements of the CCPA are sufficiently evident to enable businesses to prepare to comply with the final regulations when the Cal AG issues them, which will likely occur this fall. Accordingly, businesses should take the following steps to comply with the CCPA in advance of the January 1, 2020 deadline:

- **Confirm That Your Business is Subject to the CCPA.** Entities must determine whether they are considered a "business" subject to the CCPA. For-profit companies should keep in mind that their subsidiaries and affiliates might also be considered separate businesses with independent obligations to comply with the CCPA.

- **Determine Whether Your Business Depends on the Sale or Purchase of Personal Information.** Businesses will need to assess whether, and to what extent their disclosures of personal information to third parties falls under the broad definition of the "sale" of data. As defined to include any disclosure of data to a third party for "valuable consideration," the concept of selling data under the CCPA may encompass seemingly routine data transfers that do not include direct monetary compensation.
- **Confirm "Reasonable Security."** Evaluate cybersecurity practices consistent with industry recognized standards (with prudent consideration given to the use of encryption, multi-factor authentication, and the Center for Internet Security's Critical Security Controls).
- **Map How Your Business Collects, Shares and Sells Personal Information.** Businesses will need to identify and track internal data flows, storage and transfers (including to service providers) in order to meet their CCPA obligations. Many businesses will reconsider their approach to personal data by building processes that foster privacy by design and by default, by anonymizing data sets when possible, and by taking their data retention and destruction policies more seriously.
- **Revise Privacy Policies.** Revise both external and internal policies to properly reflect the personal information processing activities required to be disclosed under the CCPA and to express the new rights and mechanisms available to Californians to exercise those rights.
- **Enable Consumer Opt-Out of Sale of Personal Information (when applicable).** Create a separate web page to enable California residents the ability to exercise their opt-out rights to the extent the business sells their personal information.
- **Facilitate Receipt of and Response to Consumer Requests.** Develop mechanisms for accepting, tracking and verifying consumer requests, and honoring their exercise of access, deletion and opt-out rights. Companies that already comply with the GDPR will be able to leverage many of those processes.
- **Evaluate Third-Party and Service-Provider Arrangements.** Businesses should assess the nature of personal data shared with service providers and other third parties, ensure proper vendor risk management processes are in place, and revise agreements as necessary to take CCPA requirements into account. The age-old saying remains true: a company can outsource a capability, but it cannot outsource a responsibility.
- **Implement Training Program.** Ensure employees who are responsible for handling consumer inquiries understand and are trained to handle those requests in a timely, consistent and proper fashion.

What's Next? CCPA Developments, Key Dates and Status

If you've found it hard to keep up with the current state of play of the CCPA, you're not alone. The CCPA was signed into **law** on June 28, 2018 and becomes operative on January 1, 2020. At that point, businesses will be expected to provide information to consumers regarding their data privacy practices going back to January 1, 2019. As a result, businesses will need to ensure that their information retention policies extend back at least a year to ensure their ability to comply. However, the Cal AG will not begin initiating enforcement actions until six months after the final regulations are published, or July 1, 2020, whichever is sooner.

Businesses that are racing to prepare for compliance are not alone in the CCPA ecosystem, as the executive and legislative branches of the California government are also working to finalize the law and implement regulations. Specifics regarding certain obligations and requirements remain in flux, and the Cal AG has been charged with adopting regulations to clarify numerous requirements under the CCPA between now and July 1, 2020.

Prior Amendments: The California legislature continues to amend the CCPA to address various concerns from industry, clarify ambiguous provisions, and clean up sloppy language that reflects how hastily the CCPA was drafted, introduced and adopted. Since the law was initially passed, the CCPA has been amended once through **SB-1121**. SB-1121 addressed several areas of the CCPA. Specifically, the key amendments:

- Imposed a deadline of July 1, 2020, on the Cal AG to adopt regulations furthering the purpose of the CCPA, and limits enforcement by the Cal AG until six months thereafter or July 1, 2020, whichever is sooner.

- Prohibited or limited the application of the CCPA requirements to data covered by GLBA, the California Financial Information Privacy Act, HIPAA and the California Confidentiality of Medical Information Act, and *entities* covered by HIPAA and the California Confidentiality of Medical Information Act (to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information).
- Clarified that the definition of "personal information" only applies to information that "identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household."
- Removed the requirement that a consumer give the Cal AG notice within 30 days that an action has been filed prior to continuing to pursue the action. The Cal AG's right to prohibit the private action was also removed.

Pending Amendments: In addition, six amendments have been approved by the California legislature and await the governor's likely approval by October 13, 2019. The amendments clarify critical ambiguities in the statute (but leave many others unresolved) as follows:

- ***Data Brokers.*** **AB 1202** would require "data brokers"—defined as businesses that knowingly collect and sell to third parties the personal information of a consumer with whom the business does not have a direct relationship — to register with the Cal AG for publication on the Cal AG's website. Entities regulated by the GLBA, FCRA or the California Insurance Information and Privacy Act are excluded from this provision.
- ***Employee Coverage Limitation and Training.*** Notably, **AB 25** provides that, until January 1, 2021, personal information that is collected by a business in the course of a person "acting as a job applicant to, employee of, owner of, director of, officer of, medical staff member of, or contractor of that business," will not be subject to the CCPA requirements, except the CCPA's provisions requiring notice prior to collection and providing a right to bring a private right of action based on a data breach. Among other things, AB 25 also expands the scope of information and rights that personnel responsible for handling privacy inquiries need to be trained on, and provides that businesses may require consumers to submit requests through an online account the consumer maintains with the business.
- ***Vehicle Information Exemption and Deletion Exception.*** **AB 1146** provides for an exemption from the "right to opt out, for vehicle information or ownership information retained or shared between a new motor vehicle dealer and the vehicle's manufacturer, if the information is shared for the purpose of effectuating or in anticipation of effectuating a vehicle repair covered by a vehicle warranty or a recall." AB 1146 also provides for an additional exception to a consumer deletion request for "personal information that is necessary for the business to maintain in order to fulfill the terms of a written warranty or product recall conducted in accordance with federal law."
- ***Definition Amendments (Personal Information and Publicly Available Information).*** **AB 874** amends the definition of "publicly available information" to remove a condition related to government use, further clarifying that it is not personal information. AB 874 also amends the definition of "personal information" to insert "reasonably" in front of "capable of being associated with" to provide additional contours around the broad definition of "personal information."
- ***Personal Information and Discrimination.*** **AB 1355** provides for a host of amendments and revisions to the CCPA. Among other things, AB 1355 clarifies that:
  - the standard for determining if a business may discriminate against a consumer for exercising their rights under the CCPA is if the differential treatment is reasonably related to value provided to the business by the consumer's data.
  - identified data is excluded from the definition of personal information.
  - a privacy policy must also describe consumer rights of deletion and access, instead of just describing consumer rights to understand collection, disclosure and sale activities, and discrimination prohibitions. In addition, a privacy policy need only identify that a consumer has a right to request "specific pieces of personal information" rather than requiring a business to disclose "specific pieces of personal information" within a privacy policy.
  - a business does not have personal information collection and retention obligations outside of its normal business practices.

- a "verifiable consumer request" is also required for consumer requests for access and deletion before a business obligation to respond arises.
- there is a limited exemption for personal information reflecting a written or verbal communication or a transaction between a business and a consumer in certain circumstances.
- specific activity conducted pursuant to the Fair Credit Reporting Act is exempt from the CCPA.

- ***Disclosure Methods.*** **AB 1564** provides that "a business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information is only required to provide an email address for submitting requests for information required to be disclosed" rather than a toll-free phone number. In addition, if the business maintains an internet website, the business is only required to make the internet website address available to consumers to submit requests for information required to be disclosed.

Conclusion

With the holiday season approaching, the number of productive business days between now and January 1, 2020 is rapidly decreasing. Businesses that have not already begun compliance would do well to begin preparations immediately.

To the extent a business already has implemented certain processes under the GDPR, it should leverage those procedures (and the accompanying lessons learned) as tailored to the specific requirements for, and demands of, California residents. For example, data mapping exercises and records of processing completed under the GDPR can provide a business with a head start in identifying the categories of information it collects, the purposes for which that data may be disclosed, the security and retention relating to that data, and the third parties to which such personal information is disclosed. In addition, mechanisms implemented to receive and process data subject requests could be used for the same activity under the CCPA. Obviously, there will be some tweaking necessary to ensure that the consumer rights being identified are consistent with the rights provided to consumers under the CCPA (and not the GDPR), but GDPR-compliant businesses will not need to create a compliance program from the ground up. In contrast, companies that have not suffered through GDPR growing pains will find the CCPA to be more of a challenge.

Finally, the evolving nature of the CCPA requires companies to keep track of new developments and to build flexibility into their CCPA implementation plans. White & Case continues to monitor proposed changes to the Act while awaiting the California Attorney General's forthcoming regulations. Please continue to check our California Consumer Privacy Act Guide **website** for more information.

White & Case LLP
701 Thirteenth Street, NW
Washington, District of Columbia 20005-3807
United States
T +1 202 626 3600

NY0919/PRI/M/CA/1017942/2