Articles + Publications | November 12, 2024

Practical Approaches to the CCPA

WRITTEN BY

Kim Phan | Theodore P. Augustinos

The California Consumer Privacy Act of 2018 (as amended, including by the California Privacy Rights Act, the CCPA) was drafted by a privacy rights activist, initially passed and later amended multiple times by the California legislature, and ultimately amended by referendum. It shows. The statute will continue to present challenges to organizations doing business in California, regardless of industry, as any available exemptions are limited for businesses that meet the applicability thresholds.

This article reviews common, practical challenges presented by the CCPA, and offers suggestions for addressing them practically.

1. How to work with oddly defined terms?

The CCPA adopted terminology that is unique and presents difficulties for compliance. For example, most English speakers have a firm understanding of the meaning of common terms such as “consumer,” “sell,” and “share.” These terms are defined in the CCPA, however, to defy commonly understood meanings.

For purposes of developing disclosures and processes for CCPA compliance, the business should use the terms of the statute rather than adopting terminology that might make more sense and would be consistent with other privacy laws. Note that other state comprehensive consumer privacy laws adopted to date use terminology and definitions consistent with each other, and with the European Union General Data Protection Regulation (GDPR), but they differ from the CCPA. Treating California separately should make it as easy as possible for a regulator or plaintiffs’ lawyer to determine that the business’s CCPA disclosures are clearly and completely compliant.

2. Do we really need disclosures by category?

Many businesses struggle with the presentation of their CCPA disclosures. Other disclosures, such as those required for compliance with other states’ comprehensive consumer privacy laws or the Gramm-Leach-Bliley Act (GLBA) can be streamlined and relatively simple. The CCPA however, is uniquely granular in its disclosure requirements, but offers no model or template language as guidance. For example, in regulations adopted pursuant to the CCPA by the California Privacy Protection Agency (the CPPA), Section 7011(e)(1)(E) requires the privacy policy to disclose “for each category of personal information . . . the categories of third parties to whom the information was sold or shared.” Subsection (I) requires disclosure “for each category of personal information . . . the categories of third parties to whom the information was disclosed.”

Similarly, Section 7012(e)(3) of the CPPA regulations requires the Notice at Collection to include “whether each category of personal information . . . is sold or shared” and in Subsection (4), the retention period for each

category. Subsection (e)(2) could also be interpreted to require category by category disclosure of "purpose(s) for which the categories of personal information . . . are collected and used."

If any of these would be the same for each category, a simple, consolidated statement could be offered. For example, the general statement, "We do not sell or share your personal information" should obviate the need to provide a separate, similar disclosure by category.

In contrast, the categories of third parties to whom personal information is disclosed often varies by category of personal information. In that case, it would be more difficult and may be less clear, to try to satisfy the requirement of Section 7011(e)(1)(I) of the CPPA regulation quoted above with a general statement. Therefore, a tabular format may be the simplest and most clearly compliant way to present some of the required disclosures. Although a business may view a voluminous table presenting CCPA disclosures as unwieldy, it is important to keep in mind the most likely, interested readers: the CPPA and plaintiffs' lawyers. Therefore, the checkbox approach to compliance may be the safest for compliance purposes, even though it might not impress the business's marketing department.

3. Can the CCPA disclosures integrate with other privacy disclosures?

Many businesses wrestle with how to present the various notices and policies required by different federal, state, and foreign requirements, including the CCPA. Craving simplicity and clarity, many businesses attempt to develop one set of disclosures that would address all applicable requirements. Depending on the industry and scope of the business, this could mean trying to consolidate disclosures for California and other states, the GDPR and privacy laws of other jurisdictions, and (depending on industry) the GLBA privacy requirements for the financial services industry, or the Health Insurance Portability and Accountability Act (HIPAA) privacy requirements for the healthcare industry. The terms and applicability of all these requirements are different, and they apply differently (or not at all) to different sets of individuals.

Many global or national businesses choose to extend consumer rights required by one jurisdiction to all individuals, wherever resident, and regardless of the particular relationship with the business. For example, businesses that operate in the E.U. and the U.S. may choose to extend rights extended to E.U. data subjects under the GDPR to U.S. data subjects. In that case, a business could consolidate various disclosures, such as a GDPR disclosures with various state disclosures. Others decide to extend rights, and to provide disclosures, only where legally obligated, and therefore maintain clear and distinct privacy notices and policies for specific populations and purposes.

Where such privacy disclosures apply to different sets of individuals, types of information, and types of relationships between the business and a particular individual, however, it may be better, clearer, and easier to manage if the business provides different disclosures for these different purposes. For example, every financial institution (including banking, insurance, and securities firms) that is subject to the GLBA privacy rule must have a GLBA consumer privacy notice and, in some cases, additional financial privacy disclosures under the California Financial Information Privacy Act ("CalFIPA"). If subject to the CCPA, then they would also need to provide privacy disclosures to California residents who may be personnel or business contacts, and therefore outside the scope of the CCPA's exemption for information collected subject to the CCPA. The population needing the GLBA disclosures would be completely distinct from the population requiring the CCPA disclosures. Combining the two

could result in one, longer, less clear disclosure than maintaining two clear, and specifically targeted, disclosures.

In addition, the various industry regulators have adopted a safe harbor model form for the consumer privacy notice that satisfies the GLBA requirements. To take advantage of the safe harbor, the form cannot be changed (other than in very limited, specified ways). One permitted change is the inclusion of "Other Information" in the designated section at the end of the form. This section is commonly used to address state insurance privacy disclosure requirements, leveraging the GLBA safe harbor form without jeopardizing the safe harbor. Including the voluminous CCPA disclosures in the "Other Information" section at the end of the GLBA safe harbor form, however, would seem to overshadow the CCPA disclosures, as they would be at the very end of a notice that only applies to consumers whose personal information is exempt from the CCPA. Therefore, a business could not practically combine the disclosures required by the GLBA with CCPA disclosures, without either losing the benefit of the safe harbor, or burying the CCPA disclosures.

Similarly, an online privacy policy applies to any user of the website or mobile application, regardless of where the user is resident, and regardless of any other relationship between the business and the user. The collection of information online, and the processing of that information, is often very different from the collection and processing of information collected in other contexts. For example, disclosures of online tracking technologies and the collection of IP addresses may be irrelevant to a business-to-business contact who engages with the business through email, by phone, or in person. Similarly, the CCPA required disclosures of the collection and use of sensitive personal information usually collected from personnel would be irrelevant to the typical website user (other than personnel).

In addition, the business may decide not to extend consumer privacy rights (such as rights of access, deletion, and correction) to every online user, but only to residents of jurisdictions that provide these rights. Disclosures of rights that do not apply to a particular user may be confusing or frustrating to the online user. Instead, privacy rights could be described in specific, clearly labeled disclosures that are available to the appropriate, targeted population, and not merged into or appended to a disclosure document of general applicability.

Because of the specific scope and requirements of the CCPA, separate CCPA disclosures may be developed to avoid the risks of a general, consolidated privacy disclosure.

4. When to revisit and update?

Under the CCPA, the CCPA privacy policy must be reviewed at least annually, and businesses should reflect the most recent effective date no older than 12 months old at the top of the policy itself. Internal workstreams, however, should involve privacy professionals who can flag plans to process information in new ways, or new types of information, that would not be adequately disclosed under existing disclosures. Part of this process should include the updating of all appropriate privacy disclosures to accommodate the new information or processing activities, and to demonstrate the ongoing compliance process.

* * * * *

The CCPA presents ongoing compliance challenges, required to be revisited every year by businesses subject to the CCPA, with disclosures to be updated sooner if and as processing activities change. Due to unique

terminology and requirements for disclosures, the CCPA stands alone among other privacy requirements, presenting challenges for businesses, especially those required to satisfy the privacy requirements of multiple jurisdictions and industry sectors. A thoughtful approach to content and presentation of CCPA disclosures may help satisfy compliance obligations and avoid potential confusion, even if maintaining separate disclosures specific to the CCPA may increase the number and volume of privacy disclosures.

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- Privacy + Cyber