Analysis

What to Write When Rewriting a Calif. Privacy Policy

Mark E. Smith
CIPP/US, CIPP/C, CIPM
Bloomberg Law Legal Analyst

Bloomberg Law

What to Write When Rewriting a Calif. Privacy Policy

By Mark E. Smith, CIPP/US, CIPP/C, CIPM, Bloomberg Law Legal Analyst

An organization's public-facing privacy notice (a.k.a., its privacy policy) is arguably the most important document that no one ever reads. No one in the purported audience, that is. Notwithstanding the stated intent of the California Privacy Rights Act (CPRA) to "help consumers become more informed" about data collection and management practices, the cynic in me suspects that the primary readers of any company's privacy policy will be the regulators.

And given the CPRA's creation of the California Privacy Protection Agency—a new regulatory body with a $10 million annual budget—drafters of privacy policies would do well to write with this audience, and its potential enforcement powers, in mind.

Prologue

Approved by voters as the next chapter to the California Consumer Privacy Act (CCPA), the CPRA makes considerable revisions to consumer rights and business obligations, most of which will not become operative until Jan. 1, 2023.

I have already addressed the CPRA's changes to the notice at collection and the notice to opt out. It's time to tackle the most important—and most wordy, most tedious, most exhaustive, and most tiresome—notice of them all: the privacy policy. A page-turner it is not. Yet the CPRA's enhancements will require edits to your prose before regulatory reviewers commence scrutiny of your policy.

Character Development

Like any good novel, the privacy policy introduces key characters to advance the action, and the principal players in a California privacy policy are undoubtedly the rights afforded consumers. At its core, the privacy policy must describe those rights in some detail, along with the methods for consumers to exercise them.

As I explained before, the CPRA not only bolsters the scope of consumer rights created by the CCPA, but it also introduces new ones. Specifically, it broadens existing rights to encompass the "sharing" of personal information with third parties, and it creates new rights to correct inaccurate personal information and to limit the use of sensitive personal information.

Therefore, a CPRA-enhanced privacy policy will need to account for these developments, along with an explanation of what "sharing" and what "sensitive personal information" is.

Conflict Resolution

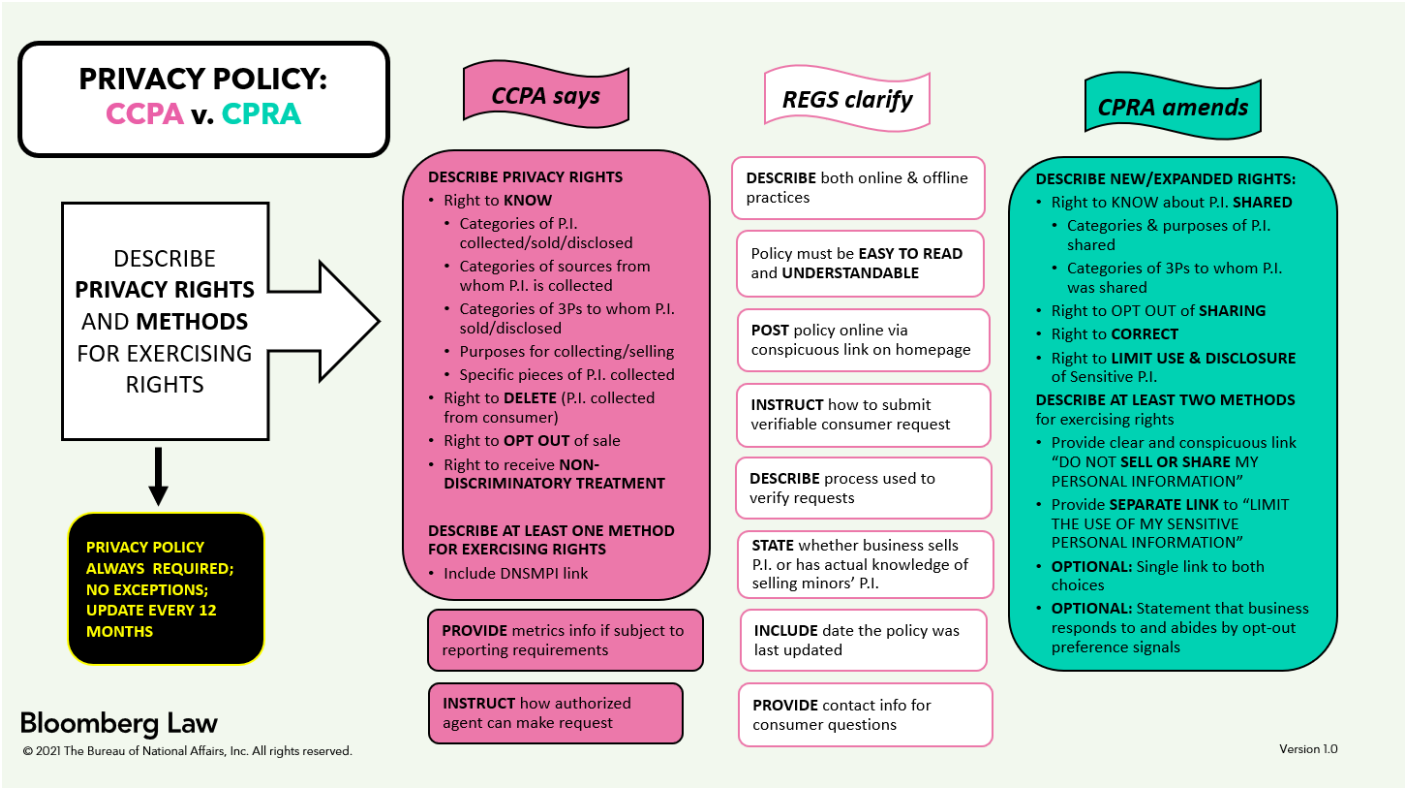
A privacy policy must also describe specific methods for consumers to exercise their rights. Under the CCPA, however, the number of options to make available has been unclear.

As currently written, the CCPA indicates that the privacy policy must include "one or more" designated methods for consumers to exercise their rights, specifically in reference to the right to know and the right to delete. See Cal. Civ. Code §1798.130(a)(5)(A).

Elsewhere, the CCPA states that businesses must provide "two or more" designated methods for submitting requests. See Cal. Civ. Code §1798.130(a)(1)(A). That provision, however, refers solely to the right to know and does not specifically mention that those methods must be included in the privacy policy.

While not quite a cliffhanger, businesses following the CCPA storyline were left to wonder if just one method for deletion requests would be sufficient.

In a move that some may consider anticlimactic, the CPRA modifies subsection (a)(5)(A) to require "two or more" designated methods in the privacy policy, and it supplements subsection (a)(1)(A) with a specific reference to requests for deletion (along with the new right to correction).



Plot Twist

Despite that resolution, the CPRA adds an element of would-be suspense of its own, through its (most likely inadvertent) deletion of a recently added privacy policy requirement.

Superfans of California privacy may recall a measure approved by Gov. Gavin Newsom last September (AB 713) that aligned certain CCPA exemptions with the federal Health Insurance Portability and Accountability Act (HIPAA). Among other things, AB 713 broadened the CCPA's exemptions for health data by harmonizing the CCPA's definition of "deidentified" with HIPAA.

Knowing that the CPRA could be placed on the November ballot, proponents of AB 713 tucked their clarifying text into two new sections of the California Civil Code—§1798.146 and §1798.148—thus shielding their language from potential CPRA revisions.

However, AB 713 also added a new provision to the CCPA's privacy policy requirements—specifically, subsection (a)(5)(D) of §1798.130—which requires any business that sells or discloses deidentified patient information to state whether it had used HIPAA's "expert determination method" (45 C.F.R. § 164.514(b)(1)) or HIPAA's "safe harbor method" (45 C.F.R. § 164.514(b)(2)) to deidentify the patient information.

Unsurprisingly, that provision does not appear in the CPRA; after all, it was added to §1798.130 more than nine months after the ballot measure was drafted. And since the terms of the CPRA revise and replace *all* of §1798.130, subsection (a)(5)(D) will disappear come Jan. 1, 2023.

Unless, of course, an amendment is passed in the meantime.

I find it hard to fathom that such an amendment would be introduced. Would anyone (aside from a regulator) really care which deidentification method was used? Nevertheless, businesses selling deidentified patient information better ensure that their policies currently disclose the method used, since that requirement is currently in force.

Prominent Setting

A more significant CPRA amendment affects businesses that do not sell personal information.

Under §1798.130(a)(5)(C)(i), such businesses are relieved of the requirement to display a "Do Not Sell My Personal Information" link, provided they affirmatively state in their privacy policy that they do not sell personal information.

The CPRA, which expands the scope of the provision to cover businesses that do not "share" personal information, maintains the same exemption: There's no need to display a "Do Not Sell or Share" link, provided the business discloses that fact in the privacy policy.

However, the CPRA adds a single word to the clause that may require a privacy policy reassessment: it provides that the business must "**prominently** disclose that fact."

Whether "prominent" disclosure would require boldface, a larger font, or "above the fold" messaging is anyone's guess until the California Privacy Protection Agency issues regulations clarifying the matter. Those regulations are not due until July 1, 2022.

Epilogue

One storyline the CPRA has *not* changed is the one that has perplexed me from the start: the requirement to convey all of the above information in the privacy policy as well as in any California-specific description of consumers' privacy rights. Cal. Civ. Code §1798.130(a)(5).

While some stories are worth reading twice, in my view, a business's data management practices is not one of them. I'd recommend folding any California-specific content within the policy itself. Save retelling for a yarn worth repeating.

For more Bloomberg Law Analysis, visit https://news.bloomberglaw.com/bloomberg-law-analysis/.