Data Privacy and Cybersecurity

California Privacy Protection Agency to Start Formal CPRA Rulemaking Process

By: Madeleine V. Findley and Benjamin T. Hand

On June 8, 2022, the California Privacy Protection Agency ("CPPA" or "Agency") voted to begin the formal rulemaking process for regulations implementing the California Privacy Rights Act (CPRA). The Agency Board discussed and approved draft proposed regulations and an Initial Statement of Reasons that were posted on the Agency's website on May 27, 2022 and June 3, 2022, respectively. These draft regulations—which will be subject to public comment and revision before they become final—provide important guidance on implementation of significant provisions in the CPRA regarding, for example, sensitive consumer personal information, opt-out links, mandatory recognition of opt-out preference signals, and additional topics. A high-level summary of the proposed regulations is provided below.

First, an important caveat: these draft regulations do not cover every topic on which the CPRA tasked the Agency with adopting regulations. The draft notably does not address how businesses should conduct privacy risk assessments, cybersecurity audits, or provide access/opt-out rights to consumers regarding the use of automated decision-making technology (including profiling). Nonetheless, the 66 pages of proposed draft regulations contain important guidance on and illustrative examples of a number of key issues, including likely requirements for opt-out links, recognition of opt-out signals, and obtaining consumer consent without being "manipulative." The draft regulations are detailed, technical, and prescriptive, which will increase compliance costs for businesses operating in California.

Collection and Use of Personal Information. The draft regulations specify that a business' collection, use, and/or sharing of a consumer's personal information "shall be reasonably necessary and proportionate to achieve the purpose(s) for which the information was collected." (§ 7002). "[R]easonably necessary and proportionate" must be "consistent with what an average consumer would expect" when the consumer's personal information was collected. Before a business may use the consumer's personal information for an unrelated or incompatible purpose, it must obtain the consumer's explicit consent.

Consumer Disclosure Requirements. Businesses will be required to provide all disclosures to consumers, including descriptions about how to exercise consumer data rights in easy-to-read and understandable language, and avoid confusing or manipulative language. (§ 7003). In addition to the familiar requirements for disclosures that must appear in privacy policies, the proposed regulations provide that the privacy policy must state whether the business discloses sensitive personal information for purposes other than those authorized by CPRA. If so, the business must provide notice of the right to limit or opt-out of such disclosure. (§ 7011).

Consumer Choices and Dark Patterns. Additionally, businesses must make consumer choices regarding their personal information symmetrical, meaning that the steps for exercising a privacy-protective choice shall not be longer or more complicated than the steps to exercise a less privacy-protective choice. (§ 7004). Methods that do not comply with these requirements may be considered a "dark pattern" and consumer agreements obtained through dark patterns shall not constitute consumer consent.

Do Not Sell or Share My Personal Information. A business that sells or shares consumer personal information must provide notice and give consumers a way to opt out of such sale or sharing. (§ 7013). That can be a clear and conspicuous "Do Not Sell or Share My Personal Information," or the alternative "Your California Privacy Choices" link and opt-out icon, located in either the header or footer of the business' internet homepages. A business that collects personal information through an app or device must provide notice "in a manner that ensures the consumer will encounter the notice while using the [app or] device."

Opt-Out Preference Signals. The draft regulations appear to require a business to recognize opt-out preference signals, which would permit a consumer "to opt out of sale and sharing of their personal information with all businesses they interact with online without having to make individuated requests with each business." (§ 7025). A business may also "process opt-out preference signals in a frictionless manner" to allow consumers to opt out of the sale or sharing of their personal information. The regulations do not reference any specific "opt-out preference signal," but require the business to explain in their privacy policy how and when they process opt-out signals.

Limit the Use of My Sensitive Personal Information. Similarly, a business that collects and uses a consumer's sensitive personal information must provide notice and provide consumers with a way to limit such use. (§ 7014). This can be a clear and conspicuous "Limit the Use of My Sensitive Personal Information" link in the header or footer of the business' internet homepage, or—for apps or devices—in a manner that ensures the consumer will encounter the notice while using the app or device.

Notice at Collection. The draft regulations also specify additional disclosures that businesses must include in their notice at collection of personal information. (§ 7012). Two are particularly worth noting. *First*, a business must list the categories of sensitive personal information the business has collected, and whether it is sold or shared. *Second*, a business that allows third parties to control the collection of personal information must list the names of all such third parties or describe their business practices. The draft regulations provide several examples, including a business that allows an analytics company to collect consumers' personal information on the business' website, and would require the business to identify the analytics company in its notice at collection or describe the analytics company's information practices.

Consumer Rights Requests. The draft regulations also offer guidance on consumer requests. First, the draft regulations modify the existing right to delete personal information. (§ 7022). Importantly, when a consumer requests deletion, a business must not only permanently delete personal information as requested but must also instruct its service providers and contractors to delete the information in their systems. Additionally, a business also must provide consumers with a means of requesting correction of inaccurate personal information and instruct service providers and contractors to do the same. (§ 7023).

Service Provider Agreements. Additionally, the draft regulations provide guidance on the terms that a business must include in its agreements with service providers and contractors, including, for example, prohibitions on combining personal data received from the business with personal information received from another source. (§ 7051).

Next Steps. The CPPA will submit its Notice of Proposed Rulemaking Action, accompanied by the Initial Statement of Reasons, to the Office of Administrative Law. Once published in the California Regulatory Notice Register, and on the Agency's website, the formal public comment period will begin and is expected to last 45 days. This means, as expected, that final regulations will not be ready by the July 1 deadline in the statute. The initial public comment period will likely be followed by public hearing(s), an additional public comment period of at least 15 days, and then a board meeting to vote to approve final regulations and a Final Statement of Reasons.

Contact Us

Madeleine V. Findley
mfindley@jenner.com | Download V-Card

Benjamin T. Hand
bhand@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

David Bitkower
Co-Chair
dbitkower@jenner.com
Download V-Card

Madeleine V. Findley
Co-Chair
mfindley@jenner.com
Download V-Card

Shoba Pillay
Co-Chair
spillay@jenner.com
Download V-Card