Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

CPPA Issues Its First Draft of CPRA Regulations

July 11, 2022

Companies are now on the clock for comments on the new proposed California Privacy Rights Act (CPRA) regulations. On July 8, 2022, the California Privacy Protection Agency (CPPA) filed a Notice of Proposed Action, triggering a 45-day comment period (followed by a public hearing and an additional 15-day comment period if the CPPA proposes material changes as a result of public comments) on the first set of draft regulations governing compliance with the California Consumer Privacy Act (CCPA), as amended by the CPRA ("CPRA Amendments").

The CPPA's draft regulations update the CCPA regulations promulgated by the California Attorney General,[1] with the goal of harmonizing requirements under the CCPA with new rights and concepts introduced by the CPRA Amendments.[2]

Though the draft regulations are far from final, they signal key compliance considerations for businesses. In particular, the extensive operational requirements for CCPA compliance detailed in the draft regulations generally provide a baseline that businesses can use to prepare for the operational changes they may need to implement. As discussed at the CPPA's June 8, 2022, board meeting, the CPPA believes that the draft regulations and the CPPA's Initial Statement of Reasons (ISOR) will provide the needed consolidation and clarification for businesses to meet their obligations under the law.

Below, we have summarized key high-level takeaways from the draft regulations and supporting materials.

Key Takeaways from Draft Regulations

Increased Transparency Requirements: Several sections of the draft regulations address the CPRA Amendments' new or expanded requirements for notices that businesses must provide to consumers. For example, in addition to existing requirements, a business's notice at collection would need to provide:

1. A list of categories of sensitive personal information to be collected.

2. Whether personal information is sold or shared.

3. How long the business intends to retain each category of personal information (or if not possible, the criteria used to determine the retention period).

Contact Information

If you have any questions, please contact a member of the Akin Gump cybersecurity, privacy and data protection team.

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Rachel Claire Kurzweil
Counsel
rkurzweil@akingump.com
Washington, D.C.
+1 202.887.4253

Lauren E. York
Counsel
lyork@akingump.com
Dallas
+1 214.969.4395

Rafita Ahlam
Associate
rahlam@akingump.com
New York
+1 212.872.8002

Tina M. Jeffcoat
Associate
cjeffcoat@akingump.com
Dallas
+1 214.969.2741

4. If the business allows third parties to control the collection of personal information, the names of all the third parties (alternatively the business can list information about the third parties' business practices).[3]

The draft regulations also introduce additional required disclosures for a business's privacy policy as well as general provisions covering how all disclosures and communications to consumers must be presented.[4]

Consent and Symmetry in Choice: In line with the CPRA Amendments, the draft regulations clarify several consent-related requirements, including that a business must obtain explicit consent if it intends to use a consumer's personal information for any purpose that is "unrelated or incompatible with the purpose(s) for which the personal information [was] collected or processed."[5]

Further, the draft regulations specify that affirmative consent methods must have "symmetry in choice,"[6] meaning that the path for a consumer to exercise a more privacy-protective option cannot be longer than the path to exercise the less privacy-protective option. This provision is intended to ensure that the consumer's choice is freely made and not otherwise manipulated, subverted or impaired through the use of dark patterns. While the draft regulations clearly prohibit the use of certain language the CPPA has expressly identified as asymmetric (using "Yes" and "Ask me later" for an opt-in instead of "Yes" and "No"), they do not otherwise explain exactly when choices become asymmetric.[7]

Notification of Third-Party Collection: The draft regulations also address instances where a first party business allows third parties to collect personal information from consumers.[8] For example, the draft regulations add a requirement that if a business allows a third party to control the collection of personal information from the business's website (through, for example, analytics cookies), then the business must:

- Notify the consumer of the names of all third parties collecting personal information on its website; or
- Provide the consumer with information about the third party's information handling practices in its notice at collection.[9]

The draft regulations also clarify that notice is required where third parties collect personal information from another business's physical location.[10] For example, if a coffee shop is providing Wi-Fi to its customers and allows the internet service provider (ISP) to collect personal information from consumers using the internet at the shop, the coffee shop must have signage directing consumers to the ISP's privacy policy.[11]

Operationalizing Right to Correct and Right to Delete: The draft regulations include specific requirements for operationalizing new consumer rights (a goal especially emphasized in the CPPA's June 8th board meeting), including a consumer's right to correct or delete personal information. For example, when handling a request from a consumer to correct inaccurate personal information about the consumer, a business may deny the request if it determines the information is more likely accurate than not, but it must consider the "totality of the circumstances."[12] These circumstances can include the nature of the personal information (whether it is sensitive, unstructured or objective), how the business obtained the information and documentation on the accuracy of the information from the consumer, the business or another source.[13] For

a request to delete personal information, businesses must notify all of their service providers and contractors to delete the personal information, as well as all third parties to whom the business sold or shared that personal information, unless this would be impossible or involve disproportionate effort.[14]

Implementation of Expanded Opt-Out Right and Right to Limit Sharing: The CPRA Amendments expanded a consumer's opt-out right to include the right to opt out of the "sharing" of personal information and included a new right for a consumer to limit a business's use of sensitive personal information. In providing guidance on operationalizing these rights, the draft regulations require that opt-out and use limitation links be conspicuous and either (1) immediately effectuate the request or (2) direct a consumer to a webpage which explains the consumer's right to opt out or limit use (as applicable) and how to exercise that right.[15] Instead of providing separate links for both opt-out and use limitation, businesses have the alternative option of providing a single, clearly-labeled link to effectuate both of these consumer rights.[16] The draft regulations specify that this link shall be titled either "Your Privacy Choices" or "Your California Privacy Choices," shall direct the consumer to a webpage with information about the consumer's opt-out and limitation rights and shall include a specified icon.[17] Notably, the draft regulations also provide further guidance on how businesses must respond to consumer opt-out preference signals, including illustrative examples and the requirement to process opt-out preference signals in a "frictionless manner." The draft regulations state that this new concept of "frictionless manner" prohibits responses to consumer opt-out preference signals from (1) charging a fee, (2) changing consumer experience or (3) displaying pop-ups or other content other than acknowledgement of the opt-out.[18]

"*Disproportionate Effort" Definition*: The CPRA Amendments added a concept of "disproportionate effort" as a limiting factor for certain consumer requests. For example, the CPRA Amendments add that in responding to a request to delete consumer personal information, the business must notify all third parties to whom the business has sold or shared such personal information to delete the consumer's personal information "unless this proves impossible or involves disproportional effort."[19] The CPRA Amendments also specify that a consumer can make a request to know beyond the CCPA's normal 12-month look-back period and a business must comply "unless doing so proves impossible or would involve a disproportionate effort."[20] As explained at the board meeting, the draft regulations attempt to clarify new CPRA-introduced concepts, such as disproportionate effort. In the context of a business responding to a consumer request, disproportionate effort means "the time and/or resources expended by the business to respond to the individualized request significantly outweighs the benefit provided to the consumer by responding to the request."[21] For example, disproportionate effort might be involved when the personal information subject to the request is not in a "searchable or readily-accessible format, is maintained only for legal or compliance purposes, is not sold or used for any commercial purpose, and would not impact the consumer in any material manner."[22]

Expanded Downstream Contracting Requirements: The CPRA Amendments require businesses to include certain provisions in contracts with entities to which the businesses disclose personal information, including service providers, contractors and third parties. As stated in the board meeting, the draft regulations revise and consolidate these existing requirements for service provider contracts and add a new

section specifically addressing contracts with non-service provider entities (i.e., contractors and third parties).[23] Notable clarifications to assist with implementating these contracts include:

- Additional examples to help determine when service providers and contractors can retain personal information they obtained in the course of providing services.[24]
- New restrictions on the types of advertising a business may provide and still be considered a service provider, including a specification that an entity providing cross-context behavioral advertising is always a third party. Additionally, a service provider or contractor contracting with a business for advertising services may not combine personal information from consumers who have opted out of the sale or sharing of personal information received within that business relationship with personal information the service provider or contractor received from outside that relationship.[25]
- Clarifications regarding the distinctive treatments of service providers, contractors and third parties for contract and due diligence requirements. Of note, the draft regulations make clear that businesses cannot describe their business purpose of data processing in "generic terms."[26] Interestingly, whether a business conducts due diligence on service providers, contractors and third parties factors into the business's ability to argue whether that service provider, contractor or third party used personal information in violation of the CCPA.[27]

Obligations of Third Parties: The draft regulations place additional requirements on third parties. For example:

- A business's contract with a third party must specify that the business is disclosing personal information to the third party for limited and specified purposes and that the third party may only use such personal information for those purposes.[28]
- When a third party collects personal information from a consumer online and receives an opt-out preference signal, that third party must recognize that signal and not use, retain or disclose that personal information unless informed by the business that the consumer has consented, or if the third party becomes a service provider or contractor.[29]
- Third parties must comply with a consumer's request to delete or request to opt out of the sale or sharing of personal information forwarded from a business that provided, made available or authorized the collection of the consumer's information.[30]
- A third party must also comply with a consumer's request to limit the use and disclosure of sensitive personal information forwarded from a business that provided, made available or authorized the collection of the consumer's sensitive personal information (unless such use or disclosure was for one of the draft's enumerated permissible purposes, such as when providing goods reasonably expected by the consumer or when detecting security incidents).[31]

Audit and Enforcement. The draft regulations grant the CPPA greater authority to investigate and enforce the CCPA. Specifically, the CPPA may initiate investigations without said investigations resulting from a sworn complaint or referred from other government agencies or private organizations.[32] It may also initiate a proceeding against an alleged violator provided there is probable cause that the "evidence

supports a reasonable belief that the CCPA has been violated."[33] Lastly, it may audit businesses, service providers, contractors and individuals to ensure compliance.[34] At its board meeting, the CPPA stressed that it views audits as an investigatory tool, similar to an administrative subpoena. The CPPA can use these audits to investigate possible CCPA violations, if a subject's collection or processing of personal information "presents significant risk to consumer privacy or security" or if the subject has a history of noncompliance in relation to the CCPA "or any other privacy protection law."[35]

Conclusion

While these draft regulations contain many substantive, sweeping alterations with substantial implications for businesses subject to the CCPA as amended by the CPRA, they will likely undergo significant modifications during the upcoming comment period.

Nevertheless, the draft regulations assist with interpreting the CPPA, including how it views businesses' obligations and how it may exercise its enforcement and audit authority. New consumer-facing disclosures, new notice obligations, new right to correct obligations, new contract requirements and other added provisions have considerable repercussions for businesses and their data practices. Businesses that have not already determined if they are subject to the CCPA (either as-is or as amended by the CPRA) should do so as soon as possible. Businesses should also consider whether they want to comment on the current draft of the regulations. The comment period closes on August 23, 2022.

[1] Prior to April 21, 2022, rulemaking authority for the CCPA was vested in the California Attorney General (AG).

[2] California Privacy Protection Agency, Draft Proposed California Consumer Privacy Act Regulations (May 27, 2022), hereinafter "Draft," available at https://cppa.ca.gov/meetings/materials/20220608_item3.pdf.

[3] *Id.* § 7012(e).

[4] *Id.* § 7011(e).

[5] *Id.* § 7002(a).

[6] *Id.* § 7004(a)(2).

[7] *Id.* The draft regulations specify that methods that do not comply with these requirements are considered dark patterns and so do not constitute valid consent (§ 7004(b)).

[8] *Id.* § 7012(g).

[9] *Id.*

[10] *Id.* § 7012(g)(3).

[11] *Id.* § 7012(g)(4)(B).

[12] *Id.* § 7023(b).

[13] *Id.* Additional details on the requirement for documentation can be found in § 7023(d).

[14] *Id.* § 7022(b).

[15] *Id.* § 7013(c),(e); § 7014(a),(c).

[16] § 7013(d); § 7014(d); § 7015(a).

[17] § 7015(a)-(b). The icon is the same one specified in the earlier CCPA draft regulations and is to be placed at the left or right of the title.

[18] *Id.* § 7025(f).

[19] Cal. Civ. Code § 1798.105(c)(1).

[20] *Id.* § 1798.130(2)(B).

[21] Draft at § 7001(h).

[22] *Id.*

[23] *Id.* § 7051(a)-(e); § 7053(a)-(e).

[24] *Id.* § 7050(b).

[25] *Id.* § 7050(c).

[26] *Id.* § 7051(a)(2); § 7053(a)(1).

[27] *Id.* § 7051(e); § 7053(e).

[28] *Id.* § 7053(a)(2).

[29] *Id.* § 7052(c).

[30] *Id.* § 7052(a).

[31] *Id.* § 7052(b); § 7027(l).

[32] *Id.* § 7301.

[33] *Id.* § 7302.

[34] *Id.* § 7304(a).

[35] *Id.* § 7304(b).