Global Privacy Controls & the Road to CPRA

August 2021

Table of Contents

I. Introduction

In November 2020, California voters enacted the California Privacy Rights Act (CPRA) by ballot initiative. The new law builds on the existing California Consumer Privacy Act of 2018 (CCPA), which provides consumers with rights to access, delete, and opt out of the sale of their personal information. The ballot initiative expands these rights and adds new obligations and limitations on how businesses can collect, use, and disclose California consumers' personal information. The CPRA's substantive provisions go into effect January 1, 2023.

A hallmark of the new CPRA is its expansion of consumer choices first introduced into law by the CCPA. Where the CCPA guaranteed a right to opt out of the sale of personal information, the CPRA adds a right to opt out of "sharing" of personal information in the context of cross-context behavioral advertising, and includes a new right to limit how a business uses or discloses sensitive personal information.

While it expands the consumer opt-out right, the CPRA also provides a business with an alternative to offering such rights. The business can dispense with the "Do Not Sell/Share" button(s) if it honors lawful opt-out preference signals sent by a "platform technology or mechanism," which we refer to as global privacy controls (GPCs). Indeed, a GPC that meets the CPRA's requirements will provide each consumer with the ability to send an opt out preference signal but leaves the details of GPCs undefined pending regulatory input on technical specifications and operational considerations. Through the CPRA regulatory process, there will be an opportunity to issue comments on these points and to help ensure that when consumers use a mechanism such as a GPC, they have clearly expressed their preferences through clear and understandable settings and without unfair manipulation by pre-selected default choices as part of a unified technical solution.

This white paper provides an overview of GPCs as addressed by the CPRA, discusses technical and implementation considerations raised by the new law, compares the CPRA approach with that of the CCPA, and outlines technical and other considerations being considered by the IAB Tech Lab to address as a prerequisite to successful implementation of GPCs.

II. The Legal Basis for GPCs under California Law

The CPRA expressly endorses GPCs as one mechanism for consumers to express their opt out preferences. This section provides background on the context and legal basis under the CPRA for GPCs as a solution for businesses to solicit consumer opt out preferences.

A. Background on Opt Out Rights

The CPRA grants consumers the right, at any time, to direct a business that “sells” or “shares” personal information about the consumer to third parties not to sell or share that data.[1] When a consumer opts out, a business is prohibited from selling or sharing the consumer’s personal information on a going forward basis. The consumer’s decision can only be reversed if he or she later provides consent.[2]

A request to opt out can apply broadly to any sales or sharing of personal information by a business. The opt-out applies both online and offline without legal distinction.

In addition to the rights to opt out of sales and sharing of personal information, consumers will also have the right under CPRA to limit how a business uses or discloses sensitive personal information,[3] unless a consumer subsequently provides consent to the use or disclosure of such data.[4] For example, a business would not be able to use sensitive data for various commercial purposes, such as inferring characteristics of a consumer for advertising or marketing.[5] On the other hand, CPRA explicitly permits a business to continue to use sensitive data for certain business purposes, including to perform services reasonably expected by an average consumer who requests such services.[6]

For each type of opt out request, the CPRA requires a business to wait at least 12 months before requesting that the consumer consent to sales or sharing of personal information, or the use or disclosure of sensitive personal information.[7]

[1] *See* Cal. Civ. Code 1798.120(a). To “sell” remains just as broad in CPRA as in CCPA, and covers disclosures of personal information by a business to a third party for monetary or other valuable consideration. *See* Cal. Civ. Code 1798.140(ad). To “share” refers to disclosures of personal information by a business to a third party for cross-context behavioral advertising, whether or not there is monetary or other valuable consideration. *See* Cal. Civ. Code 1798.140(ah). “Cross-context behavioral advertising” is a new defined term meaning “the targeting of advertising to a consumer based on the consumer’s personal information obtained from the consumer’s activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.” Cal. Civ. Code 1798.140(k).

[2] Cal. Civ. Code 1798.120(d); Cal. Civ. Code 1798.140(h) (defining “consent” as “any freely given, specific, informed, and unambiguous indication of the consumer’s wishes by which the consumer, or the consumer’s legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose.”).

[3] Cal. Civ. Code 1798.121(a); Cal. Civ. Code 1798.140(ae) (defining “sensitive personal information” as (1) Personal information that reveals: (A) A consumer’s social security, driver’s license, state identification card, or passport number; (B) A consumer’s account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (C) A consumer’s precise geolocation; (D) A consumer’s racial or ethnic origin, religious or philosophical beliefs, or union membership; (E) The contents of a consumer’s mail, email, and text messages unless the business is the intended recipient of the communication; or (F) A consumer’s genetic data; (2) (A) The processing of biometric information for the purpose of uniquely identifying a consumer; (B) Personal information collected and analyzed concerning a consumer’s health; or (C) Personal information collected and analyzed concerning a consumer’s sex life or sexual orientation.).

[4] Cal. Civ. Code 1798.121(b).

[5] *See* Cal. Civ. Code 1798.121(d).

[6] Cal. Civ. Code 1798.121(a).

[7] Cal. Civ. Code 1798.135(c)(4).

B. Options to Submit an Opt Out Request

CPRA further describes two options for businesses to accept opt out requests from consumers.[8] As a first option, a business may provide an opt out link on its website. Businesses can choose to provide two links – one for consumers to opt out of sales or sharing of personal information, and one to limit uses of sensitive personal information – or one link that combines the requests.[9] The other option, in lieu of these links, is for a business to allow consumers to opt out via a GPC.[10]

Importantly, the CPRA does not favor one option over the other, stating, "[a] business that complies with subdivision (a) is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b)." In other words, a business may either add opt out links to its website or recognize and respond to a GPC, at its option.[11] However, a valid GPC must provide the same functionality as opt out links, giving the consumer the ability to fully opt out of the sale or sharing of personal information or to limit the use or disclosure of sensitive personal information.

The CPRA further states that the technical specifications for GPCs are to be addressed in CPRA rulemaking proceedings.[12] Broadly, the regulations will provide detail on how a business that elects to comply with a GPC should respond to GPC signals and provide consumers with options to modify their opt out preferences,[13] along with other implementation and technical requirements.[14] The rulemaking process to finalize the CPRA regulations may begin as early as the summer of 2021, with a target completion date of July 1, 2022 for final rules.

[8] Cal. Civ. Code 1798.135(a), (b).

[9] Cal. Civ. Code 1798.135(a)(2), (3).

[10] Cal. Civ. Code 1798.135(b).

[11] Cal. Civ. Code 1798.135(b)(3).

[12] Cal. Civ. Code 1798.135(b)(1); Cal. Civ. Code 1798.185(a)(19), (20).

[13] Cal. Civ. Code 1798.185(a)(20).

[14] Cal. Civ. Code 1798.185(a)(19).

III. Legal and Operational Considerations for Companies Choosing to Accept GPCs

This section addresses legal and operational considerations that will necessarily influence whether a business chooses to accept GPC signals. These issues include obligations around identity verification, consent, safeguarding consumers' interests and competition, and procedures for consumers to modify their opt out preferences.

A. Identity Verification

Businesses implementing GPCs (or any opt out) should consider what information about the individual consumer is functionally necessary and legally required to fulfill the opt out. Whereas a business may be able to use online identifiers on a pseudonymous basis to suppress cross-context behavioral advertising, the business might have difficulty suppressing offline sales of personal information or linking a request to sensitive personal information data points without knowing the identity of the requestor.

As a privacy law designed, in part, to advance the goal of data minimization,[15] CPRA should not require a business to marry online and offline identifiers solely for the purposes of completing a privacy request, just as it does not allow a business to require a consumer to open an account to complete a privacy request.[16] The CPRA states that a business can request that a consumer provide only the additional information that is necessary to fulfill the consumer's request.[17] But it is unclear how in the context of a GPC that extends to offline data a business could request enough information to identify a consumer or that such a measure would be desirable.

From a public policy standpoint, regulators should not require businesses to leverage available data that might not otherwise be merged or correlated simply to identify the consumer making an opt out request in order to effectuate that request. Some businesses that don't have direct identifiers would have to rely on probabilistic matching that leverages the power of big data to align disparate profiles. This is an inexact science that would not provide a business with the ability to meet legal obligations. Asking too much of this technology could, in turn, incentivize the collection of more consumer data to offset risk.

CPRA rules should also refrain from requiring the business to collect additional personal information for purposes of linking an online and offline request or requests made from different devices or with different browsers. Where a business already authenticates a user or uses deterministic matching based on its knowledge of a consumer identity, the business may be able to link online and offline identities seamlessly. But the CPRA does not support requiring businesses to use account-based authentication or collect additional information beyond what is "necessary" to fulfill a request.[18] Collection of additional personal information simply to link online and offline identifiers is inconsistent with this principle.

[15] *See* Cal. Civ. Code 1798.100(c) ("A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.").

[16] Cal. Civ. Code 1798.135(c)(1) ("A business that is subject to this section shall: … Not require a consumer to create an account or provide additional information beyond what is necessary in order to direct the business not to sell or share the consumer's personal information or to limit use or disclosure of the consumer's sensitive personal information.").

[17] Cal. Civ. Code 1798.135(c)(1).

[18] Cal. Civ. Code 1798.135(c)(1).

Ultimately, the CPRA regulations can clarify these issues and provide businesses that collect, sell, or share online identifiers with the option to satisfy their obligations by using online-only GPC signals.[19] Regulations can also make clear that a business would not have an obligation to associate online identifiers with offline data, or to try to link different devices, unless it already does so through a consumer account as part of the business's existing practices.

B. Manifesting Consent in the Context of GPCs

Instead of only permitting consumers to opt out on the digital property of each business, the CPRA goes further in permitting consumers to use a GPC to communicate that preference, but only if the consumer first consents to opting out through the GPC.[20] Rather than the opt out approach reflected elsewhere in the CPRA, the requirement of consumer consent to use a GPC reflects a definition of consent that borrows from concepts in the EU General Data Protection Regulation (GDPR) that consent must be a "freely given, specific, informed, and unambiguous indication of the consumer's wishes," which may be given "by a statement or by a clear affirmative action.[21]

These consent concepts have specific meanings that will become central to operationalizing GPCs:

- "Freely given" indicates that the consumer is free to choose preferences without recourse or facing discrimination for those choices.
- "Specific" and "informed" indicates that the consumer should be provided a clear, separate notice with an explanation of how the GPC operates, and detail on the meaning and import of submitting an opt out request.
- "Unambiguous" indicates that the consumer's action was intentional and affirmative. For example, we would expect to see emerging consensus on legal language where the consumer can certify and digitally sign his or her decision to opt out.

This high bar for consent, which is required for the use of GPCs, stands in contrast to today's browser-based preferences that are often described in a cursory manner or that use default settings. Instead, GPC developers will be required to provide a clear notice to the consumer and obtain his or her unambiguous consent to enable the GPC. The business is, in turn, responsible for responding to GPC tools that appropriately collect consumer preferences on the basis of consent.

[19] Similarly, CPRA provides an option for online-only businesses to accept consumer access requests solely via email (as opposed to toll-free number plus an additional method). Cal. Civ. Code 1798.135(a)(1)(A).

[20] *Compare* Cal. Civ. Code 1798.135(b)(1) ("…an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism…") and Cal. Code Regs. tit. 11 § 999.315(c)(1) ("…clearly communicate or signal that a consumer intends to opt-out…").

[21] Cal. Civ. Code 1798.140(h).

While the CPRA sets consent standards, it does not specify the exact mechanism or technology needed to obtain consent for use of a GPC to express an opt-out preference. The CPRA, however, outlines specific procedures and contracts that do not satisfy the consent standards. These are:

- Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information;
- Hovering over, muting, pausing, or closing a given piece of content; and
- Agreement obtained through use of dark patterns (i.e., "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation.").[22]

To guarantee faithful fulfillment of consumer consent preferences, GPC developers and their business partners will need to avoid the above proscribed procedures. More appropriate approaches may include a layered approach that provides high-level, short-form, or pictorial informed consent notices linked to more detailed underlying text.

C. Business-Specific GPC Options

CPRA attempts to balance the GPC's global preference signal with business-specific signals tied to companies with which a consumer may have specific preferences based on the consumer's relationship with the business. In particular, the CPRA instructs that a consumer's preferences for particular businesses should not affect "the consumer's preferences with respect to other businesses.[23]

These business-specific preferences play out both initially when a consumer first indicates his or her opt out preference, as well as after the consumer opts out.[24] The statutory language referring to the initial GPC selection refers to an "opt out preference signal sent … to *the* business," not generally to all "businesses."[25] The statute also requires that the implementing regulations "provide a mechanism for the consumer to selectively consent to a business' sale of the consumer's personal information," not sales by all "businesses."[26] In these ways, the CPRA indicates that GPCs may provide consent preferences on an individual business-by-business basis. Any granular options can be presented alongside a global preference to opt out for all participating digital properties. For example, when a user opens a GPC tool for the first time, the user might receive a prompt to select preferences for specific sites of interest to the user individually as opposed to only setting global preferences. Individual site information might link to the site's privacy policy or other information to help the user make an informed choice. Regulations should not be prescriptive in this area in order to provide room for GPCs to experiment with how best to obtain user consent, including through granular site-specific controls, just-in-time requests appearing on each site, or preferences expressed during account or service registration with a particular business.

[22] Cal. Civ. Code 1798.140(h), (l).

[23] Cal. Civ. Code 1798.185(a)(19)(A)(v).

[24] Cal. Civ. Code 1798.135(b)(1) (indicating the preference is sent "to *the* business" (emphasis added), which underscores the GPC signal is specific to each business).

[25] Cal. Civ. Code 1798.135(b)(1) (emphasis added).

[26] Cal. Civ. Code 1798.185(a)(19(A)(v) (emphasis added).

The statute also provides a method for consumers to override their global GPC preferences on a business-by-business basis after submitting such global preferences. This may occur if a consumer wants to receive cross-context behavioral advertising or marketing from specific businesses, or benefits from a business's use or disclosure of the consumer's sensitive personal information.

Each business that accepts GPC signals is permitted under the CPRA to stand up a web page where an individual consumer can give consent to the business "ignoring" the GPC signal from that individual.[27] The web page would also provide the consumer the ability at any time to change their mind and revoke consent for the business to ignore the consumer's GPC signal (defaulting back to the consumer's GPC preferences).[28]

The task of specifying how this web page will function will again be left to regulators. However, the CPRA provides guidance to regulators that the web page should not be part of a popup, notice, or intrusive notice that obscures any part of a web page the consumer visits; should not coerce the consumer to click in order to receive full functionality of any products or services; and does not make use of any "dark patterns" to gain improper consent.[29] Accordingly, businesses will be able to provide a link to the consent web page, but will not be able to encourage clicking the link through the use of popups or other implicit or explicit incentives.

D. Safeguards for Consumer Interests and Competition

Contemplating that the GPC could become a common standard adopted across digital properties, the CPRA includes several safeguards designed to protect consumer interests and ensure competition, fairness, and choice in the marketplace.[30] These safeguards focus on preventing competitive harm or disadvantaging businesses that compete based on access to data, while also ensuring that the GPC gives full effect to consumer preferences.

Among these safeguards are the following:

- **No Defaults:** The regulations should not permit the use of defaults that could misrepresent or presuppose a consumer's intent.[31] Default options are also incompatible with the obligation that the consumer "consent" when using a GPC.
- **Competition & Consumer Choice:** The regulations should strive to promote competition and consumer choice.[32] For example, the regulations may describe how to promote competition and consumer choices when competitors and consumers rely on a common GPC tool. The regulations may also address how to weigh varying commercial interests when establishing common standards for GPCs.

[27] *See* Cal. Civ. Code 1798.135(b)(2) ("A business that allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information pursuant to paragraph (1) may provide a link to a web page that enables the consumer to consent to the business ignoring the opt-out preference signal…") (emphasis added).

[28] *See* Cal. Civ. Code 1798.135(b)(2)(A).

[29] *See* Cal. Civ. Code 1798.185(a)(20)(C); Cal. Civ. Code 1798.140(l)(defining "dark patterns").

[30] Cal. Civ. Code 1798.185(a)(19), (20).

[31] Cal. Civ. Code 1798.185(a)(19)(A)(iii).

[32] Cal. Civ. Code 1798.185(a)(20)(A).

- **Prevention of Unfair Disadvantages:** The regulations should ensure that a platform, browser, or device manufacturer that sends a GPC signal will not unfairly disadvantage another business.[33] For example, a GPC should not use language or prompts that would disadvantage publishers.
- **Technology Neutral:** The regulations should strive to be technology neutral.[34] As a result, the GPC opt out preference signal will likely need to be able to be sent on any platform, technology, or mechanism available in the marketplace.
- **Prompts When Lawfully Negating GPC:** The regulations will need to address whether and what type of content or messaging a business can provide in response to or in connection with the GPC.[35] This issue is important to prevent unlawful coercion efforts to change a GPC signal.
- **Avoidance of Conflicts in Preferences:** The regulations should address ways to avoid conflicts between the GPC and other privacy settings or tools that consumers may employ.[36] This may include privacy settings already commonly in use, such as cookie banners or interest-based advertising opt outs, or existing consumer agreements as to financial incentives with a particular business.
- **Granular Choices:** The regulations should create a mechanism for consumers to selectively consent to individual business data activities without affecting the consumer's global preferences.[37]
- **Ease of Use:** The regulations should be crafted to ensure that the GPC be consumer-friendly, clearly described, and easy to use by an average consumer.[38]
- **Consumer Protection:** CPRA regulations should prohibit businesses from harming consumer interests by responding to an opt out signal by degrading functionality, charging a fee, or coercing consumers to opt back in to sales, sharing, or uses of sensitive information.[39]
- **Minors:** The regulations will need to address how to signal to a business that the user is a minor and therefore is required to opt in rather than opt out to sales or sharing of personal information.[40]

Many of these safeguards in the CPRA are expressed as instructions for regulators who will need to craft the specific requirements. For example, rather than stating that a GPC should promote competition and consumer choice, the CPRA instructs regulators to develop regulations that promote competition and consumer choice. This model ensures that the views of the electorate expressed in the CPRA ballot initiative will be implemented while also leaving the technical details to be based on views of industry, consumers, and regulators as part of the notice and comment rulemaking process. However, as a result of this process, a final CPRA-compliant version of a GPC will not be able to be completed until the publication of the final regulations, expected in mid-2022.

[33] Cal. Civ. Code 1798.185(a)(19)(A)(i).

[34] Cal. Civ. Code 1798.185(a)(20)(A).

[35] Cal. Civ. Code 1798.185(a)(20)(B)(v).

[36] Cal. Civ. Code 1798.185(a)(19)(A)(iv).

[37] Cal. Civ. Code 1798.185(a)(19)(A)(v).

[38] Cal. Civ. Code 1798.185(a)(19)(A)(ii).

[39] Cal. Civ. Code 1798.185(a)(20)(B)(i) – (iv).

[40] *See* Cal. Civ. Code 1798.185(a)(19)(B); Cal. Civ. Code 1798.120(c).

IV. Comparison with CCPA GPC

The CPRA takes a markedly different approach to GPCs as compared with the regulations promulgated under the CCPA, as exemplified most recently in action taken by California Attorney General Rob Bonta. The CPRA expressly permits, but does not require, businesses to elect to honor preference signals from GPCs, provides guidance on a host of operational considerations and recommendations for rulemaking, and clarifies how consumers may submit opt out requests via GPC.[41] This stands in contrast to the requirement to respond to signals from GPCs in the CCPA regulations, which were developed despite there being no express mention of such requirements in the statute.

According to media reports, the Attorney General's Office has begun a campaign to enforce the CCPA regulations, calling on companies to honor GPCs.[42] The Attorney General's Office also published guidance on its website that asserts, "Under law, [GPC] must be honored by covered businesses as a valid consumer request to stop the sale of personal information."[43]

At most, the basis for the CCPA's GPC regulation is, arguably, a grant of authority to the Attorney General to establish rules and procedures to facilitate and govern the submission of requests to opt out of the sale of personal information.[44] Otherwise, the CCPA does not include any description of GPCs or guidelines on operational considerations.

The CCPA regulations promulgated by the Attorney General describe GPCs as an acceptable method for submitting a request to opt out of the sale of the consumer's personal information to a business. More specifically, the GPC is described as "user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt out..."[45] Businesses that collect personal information from consumers online must accept GPCs, according to the regulations, as long as the GPC clearly communicates or signals the consumer's intention to opt out.[46]

In comparison to the GPC described under CPRA, the regulation related to recognition of a GPC under the CCPA makes it mandatory to honor GPC preference signals, lacks a direct statutory basis, does not require consumer consent, and does not include technical and implementation specifications or details that protect consumer interests and ensure competition, fairness, and choice. The CCPA regulations also do not address how to resolve conflicts between GPC and a consumer's expressed privacy preferences, in particular by not providing a requirement for the consumer to have an option to override GPC preferences on a website-by-website basis.

The new California Privacy Protection Agency will be adopting regulations in furtherance of the CPRA, and rescind inconsistent CCPA regulations. CCPA's regulations on GPCs in general – and its mandate to accept GPCs in particular – are potential candidates for rescission given the imminent adoption of new GPC regulations and the January 1, 2023 effective date of the CPRA.

[41] *See* Cal. Civ. Code 1798.135(a), (b).

[42] *See* Kate Kaye, *California's attorney general backs call for Global Privacy Control adoption with fresh enforcement letters to companies*, Digiday (July 16, 2021), https://digiday.com/marketing/californias-attorney-general-backs-call-for-global-privacy-control-adoption-with-fresh-enforcement-letters-to-companies/.

[43] California Consumer Privacy Act, Frequently Asked Questions, https://oag.ca.gov/privacy/ccpa.

[44] California Consumer Privacy Act of 2018, Cal. Civ. Code 1798.185(a)(4) (2020).

[45] Cal. Code Regs. tit. 11 § 999.315(a).

[46] Cal. Code Regs. tit. 11 § 999.315(c).

V. Options for Technical Standards

The inclusion of GPCs in CPRA presents an opportunity to evaluate the technical privacy signaling standards IAB Tech Lab developed in conjunction with the IAB CCPA Task Force. While it is by no means required that Tech Lab update or evolve its USPrivacy API for GPC, doing so could help ecosystem participants and ultimately result in more consistent end-user experiences.

If Tech Lab updates its USPrivacy API for GPC, it could take one or all of the following forms. First and arguably easiest to implement, the Global Privacy Working Group at Tech Lab could define implementation guidance to be added to the existing implementation documentation.[47] This would not require any coding updates, but would require inputs formed from policy consensus. Second, and nearly equally straightforward, the Global Privacy Working Group at Tech Lab could facilitate the transmission of GPC signals to all relevant parties by adding the GPC value in the browser to the USPrivacy API. This would be a simple pass through, but would help supply chain participants who are not able to read client-side information due to their position in the supply chain. This could be achieved through an update to the USPrivacy Consent Management Platform (CMP) API as well as the privacy string itself. For the privacy string, it would likely mean an additional character position in the string.

Finally, with additional effort, the Global Privacy Working Group at Tech Lab could develop a lightweight library for CMPs based on the implementation guidance for different GPC site-level "Do Not Sell My Personal Information" scenarios. One good reason to do this, in addition to adding the GPC signal to the USPrivacy API, is to achieve a consistent end-user experience. While the library would not provide a direct end-user interface, it would give CMPs the tools to make sure they are implementing these scenarios consistent with regulator guidance for responding to GPCs. Technically, this would look like a set of functions a CMP could employ to check for GPC values at the site-level and then define a common API response. For example, the API response may include requesting consumer input if the GPC value does not match the USPrivacy value.

[47] https://github.com/InteractiveAdvertisingBureau/USPrivacy.

VI. Conclusion

In this white paper, IAB provides background and analysis of GPCs under CPRA and CCPA to educate the digital advertising industry on these issues as market participants prepare for the shift from CCPA compliance to CPRA compliance. Additionally, this overview also provides context for technical and implementation discussions that will be a focal point during the CPRA rulemaking process expected to commence with oversight of the California Privacy Protection Agency. Successful implementation will require a thoughtful approach with feedback from industry, regulators, and consumers.

About Us

The Interactive Advertising Bureau empowers the media and marketing industries to thrive in the digital economy. Its membership comprises more than 650 leading media companies, brands, and the technology firms responsible for selling, delivering, and optimizing digital ad marketing campaigns. The trade group fields critical research on interactive advertising, while also educating brands, agencies, and the wider business community on the importance of digital marketing. In affiliation with the IAB Tech Lab, IAB develops technical standards and solutions. IAB is committed to professional development and elevating the knowledge, skills, expertise, and diversity of the workforce across the industry. Through the work of its public policy office in Washington, D.C., the trade association advocates for its members and promotes the value of the interactive advertising industry to legislators and policymakers. Founded in 1996, IAB is headquartered in New York City.

For more information, visit iab.com.