Summary of major proposed changes and possible implications for digital advertising.

I. Changes to definitions.

a. There are significant changes to the definition of "business purpose" that would affect the activities service providers or contractors would be able to undertake outside the definitions of "sale" or "sharing." Highlights of the changes include:

i. Makes explicit that ***non-personalized advertising*** based on a consumer's current interaction with a business ***is a business purpose***.
CPRA § 1798.140(e)(4). "Non-personalized advertising" is a new defined term meaning "advertising and marketing that is based solely on a consumer's personal information derived from the consumer's current interaction with the business, with the exception of the consumer's precise geolocation." CPRA § 1798.140(t).

1. "Precise geolocation" is a new defined term meaning "data that Is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of one thousand, eight hundred and fifty (1,850) feet, except as prescribed by regulations." CPRA § 1798.140(w). This is comparable to an NAI standard of 500m (=1640.42 feet) for precise vs. imprecise location information.
2. This suggests that service providers cannot undertake activities like real-time geofencing and hence they would generally be subject to consumer opt-out rights under CPRA. The NAI Code already requires Opt-In Consent for the use of Precise Location Information for Tailored Advertising or Ad Delivery and Reporting, including real-time geofencing.

ii. Makes explicit that ***"advertising and marketing services" are business purposes <u>except</u> for cross-context behavioral advertising,*** and limits how service providers/contractors can combine PI across businesses when providing advertising and marketing services. CPRA § 1798.140(e)(6).

1. "Advertising and marketing" is a new defined term meaning "a communication by a business or a person acting on the business's behalf in any medium intended to induce a consumer to obtain goods, services, or employment." CPRA § 1798.140(a).
2. "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." 1798.140(k).

3. This suggests at a minimum that using existing third-party profiles to target ads is not an activity service providers can undertake, even if that doesn't involve creating new profiles. Compare to the current IAB LSPA where service providers are purported to be able to deliver targeted ads using existing third-party data.

b. Adds the defined term **"sensitive personal information"** meaning "(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; (F) a consumer's genetic data; and (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. Sensitive personal Information that is publicly available. . . shall not be considered sensitive personal Information or personal information." CPRA § 1798.140(ae).
    i. Sensitive PI is subject to a new consumer right under CPRA to opt out of its *use* by a business, not just its sale/sharing.
    ii. Compared to the NAI's definition of Sensitive Information, this definition is broader. For example, it includes racial or ethnic origin; religion; union membership; all information about a consumer's sex life or sexual orientation; and **ALL information concerning a consumer's health.**
c. Amends the definition of **"sale"** such that only the transfer of PI from a business to a third party can constitute a sale. CPRA § 1798.140(ad).
    i. Amendments to the definition of service provider (and the new definition of contractor) clarify that service providers/contractors are not third parties.
d. Adds a definition of **"sharing"** meaning "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party ***for cross-context behavioral advertising, whether or not for monetary or other valuable consideration***, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged." CPRA § 1798.140(ah)
    i. Note that the right to opt out has been extended to cover sharing as well as selling.
e. Adds the defined term **"dark pattern"** meaning "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." CPRA § 1798.140(l).

i. This term is used in the definition of "consent" to exclude agreement obtained using dark patterns. "Consent" is a newly defined term meaning "any freely given, specific, informed and unambiguous indication of the consumer's wishes by which he or she, or his or her legal guardian, by a person who has power of attorney or is acting as a conservator for the consumer, such as by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to him or her for a narrowly defined particular purpose. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. **Likewise, agreement obtained through use of dark patterns does not constitute consent.**

ii. The main CPRA requirements around consent are for: (1) the sale or sharing of a minor child's PI; (2) for allowing the sale or sharing of PI, or the use of sensitive PI, after a consumer has opted out; (3) participation in financial incentive programs; and (4) allowing businesses to get a consumer's consent to ignore global/platform opt-out signals.

f. Adds the defined term **"profiling"** meaning "any form of automated processing of personal Information, as further defined by regulations . . . to evaluate certain personal aspects relating to a natural person, and In particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, Interests, reliability, behavior, location or movements." CPRA § 1798.140(z).

i. The use of this term appears to be limited to permitted rulemaking in connection with "access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling[.]" CPRA § 1798.185(a)(16).

g. Amends the definition of **"service provider."** CPRA § 1798.140(ag). This includes:

i. Some new language restricting SP processing to the "direct business relationship" between the business and SP.

ii. New restrictions on combining PI obtained for different entities (complicated, and not quite the same as the proposed regulations).

iii. Requiring notice to the business if the SP is using subcontractors.

h. Adds the defined term **"contractor."** CPRA § 1798.140(j).

i. The definition of "contractor" is in most respects identical to the definition of "service provider." A few differences include:

1. Service providers process PI "on behalf of" the business, while a contractor processes PI the business merely "makes available" to the contractor.

2. Contractors must include a certification made by the contractor that the contractor understands the restrictions on its processing of PI (functionally identical to SP processing restrictions).

ii. It is not clear why the definition of "contractor" was added or what meaningful difference it makes.

iii. A redline comparing the two definitions is available here.

II. Changes to opt-out provisions.

a. Under the CCPA, consumers have the right to opt out of "sales," although the scope of that opt out has been debated. Under CPRA, the scope of the opt out is expanded to cover:

i. Sharing – PI shared for purposes of **cross-context behavioral advertising** is subject to the opt out right, regardless of whether a "sale" has occurred or whether any consideration is exchanged. CPRA §§ 1798.120(a); 1798.140(ah).

ii. Use of "sensitive personal information" by a business. Consumers would be able to **limit the use** (not just the sale/sharing) **of sensitive PI "to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services[,]"** and certain other limited business purposes (including security, non-personalized advertising, maintaining/servicing accounts, and undertaking activities to verify or maintain the quality of a service). CPRA §§ 1798.121(a); 1798.140(e)(1), (4), (5), (8).

1. This is substantially different from the NAI requirements around Sensitive Information. The NAI Code requires Opt-In Consent for the use of Sensitive Information for Tailored Advertising or Ad Delivery and Reporting, which is more stringent than the CPRA opt-out requirement for those use cases. But the CPRA's definition of "sensitive personal information" is broader because it includes, e.g., ALL health information and other categories.

b. The opt-in requirements for children (aged <16) are extended to cover "sharing" as well as "sales." CPRA § 1798.120(c).

III. Changes to verifiable consumer request provisions

a. Expanded right of deletion

i. Upon receipt of a verifiable consumer request to delete PI, a business must direct all service providers, contractors ***and third parties to whom the business has shared or sold PI, to delete that PI.*** CPRA § 1798.105(c).

1. Does that mean when a third party buys PI, that third party at most has a limited license contingent on a consumer's right to deletion?

ii. Service providers and contractors must flow deletion requests down to subcontractors, but do not have to respond to requests directly to them

(when the request should be directed to the business). CPRA § 1798.105(c)(3).

b. Adds a consumer right to request **correction** of inaccurate PI.
    i. "A consumer shall have the right to request a business that maintains inaccurate personal information about the consumer to correct such inaccurate personal information[.]." CPRA § 1798.106(a)
c. Requirements around VCRs have in general been streamlined and clarified by the CPRA.
    i. CPRA would clarify that no changes to existing data retention policies are required for compliance with VCRs. CPRA § 1798.145(j); 1798.130(a)(2)(B).
    ii. Would clarify requirements around portability and use of structured data in response to access requests. CPRA § 1798.130(a)(3)(B)(iii).
    iii. Don't have to duplicate certain information for VCRs if the same information is in the privacy policy. CPRA § 1798.110(b).
    iv. Look-back period for responding to consumer requests would no longer be limited to 12 months, and would instead include all PI since inception of the law. CPRA Section 1798.130(a)(2)
    v. In general, better organization of VCR requirements compared to today's CCPA.

IV. <u>Changes to transparency provisions</u>

a. **Businesses would not be required to post opt out links** if they allow "consumers to opt-out of the sale or sharing of their personal Information and to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications set forth in regulations." CPRA § 1798.135(b).
    i. Businesses taking this approach can ask for consent to ignore such opt-out signals if they meet certain conditions (such as avoiding dark patterns).
    ii. It is far from clear how this squares with the proposed regulations' treatment of global privacy controls.
b. Information to be disclosed by "a business that *controls the collection* of PI" at or before the point of collection would be expanded. CPRA § 1798.100(a). This would include:
    i. Enhanced requirements for the notice at or before the point of collection, including:
        1. Whether identified categories of PI are sold or shared.
        2. Breaking out separate categories, purposes, and whether sold/shared for **sensitive PI.**
        3. **Retention period** by category of PI (including breakdown by category of sensitive PI).
c. Allows that a "business acting as a third party" may meet its notice at collection obligations on its own homepage (still broadly defined). CPRA § 1798.100(b).

This more clearly delineates the transparency obligations of the primary business (with whom the consumer intends to interact) and third parties. This issue is also addressed by the proposed regulations. See 999.305(d)-(e).

i. Section 1798.115(d) requiring explicit notice and an opportunity to opt out is unchanged (except it now covers sharing, too).

d. The CPRA requires businesses that use sensitive PI to post a separate opt out titled "Limit the Use of My Sensitive Personal Information." CPRA §1798.121(a)

V. Other new obligations:

a. The CPRA introduces a **data minimization requirement**: "A business's 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." CPRA § 1798.100(a)(3), 1798.100(c).

b. The CPRA would create **a requirement for reasonable security** measures: "A business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal Information from unauthorized or illegal access, destruction, use, modification, or disclosure[.]" CPRA § 1798.100(e)

c. The CPRA would create new contractual requirements for **all** disclosure of PI by a business.

i. All businesses must have a contact (even with third parties to which they sell PI) that includes purpose limitations and that requires the same level of protection of PI as the CPRA. CPRA § 1798.100(d).

ii. One possible motivation for this change could be to preserve CA consumer's rights when PI is sold to an entity not subject to CPRA.

VI. Business classification changes:

a. The CPRA contains provisions that may clarify ambiguity in the CCPA regarding which entities are characterized as the primary "business."

i. The CPRA refers to a "business that controls the collection of PI." CPRA § 1798.100(a). Note that even if publishers technically do not collect information from 3P cookies/pixels on their properties, it would be harder to argue they do not **control** such collection.

ii. The CPRA also refers to a "business acting as a third party." CPRA § 1798.100(b). A third party is not a business (or other person) with whom the consumer "intentionally interacts." CPRA § 1798.140(ai).

b. The CPRA adds a new category of entity: a "contractor." CPRA Section 1798.140(j). This new category is discussed above in section I on definitions.

VII. Enforcement:

a. CPRA would become effective on January 1, 2023, and with the exception of the right of access, shall only apply to personal information collected by a business on or after January 1, 2022.
b. The CPRA would create the California Privacy Protection Agency and give it rulemaking and enforcement authority. See CPRA § 1798.199.10 *et seq.*
c. The new agency would have independent funding. § 1798.160.
d. There is a timeline for phasing out the AG's rulemaking and enforcement responsibilities in favor of the new agency, and the start of new rulemaking activities, starting in 2021.
    i. There are extensive provisions for new rulemaking. CPRA § 1798.185.