ACLU California

CALPIRG Standing Up To Powerful Interests

CENTER FOR DIGITAL DEMOCRACY

common sense kids action®

consumer action Education and advocacy since 1971

CFA

CR Consumer Reports®

ELECTRONIC FRONTIER FOUNDATION EFF

Media Alliance

OAKLAND PRIVACY

PRC Privacy Rights Clearinghouse

October 23, 2019

Alastair Mactaggart
c/o James Harrison
Remcho, Johansen & Purcell, LLP
1901 Harrison St, Suite 1550
Oakland, CA 94612

Re: California Privacy Rights and Enforcement Act – Privacy Coalition Comments

Dear Mr. Mactaggart:

We are a coalition of eleven privacy advocacy organizations. We write to propose ways to strengthen the initiative you filed with the California Attorney General's Office on October 9: the California Privacy Rights and Enforcement Act of 2020 (CPREA).[1] It would amend the California Consumer Privacy Act of 2018 (CCPA). *See* Cal. Civil Code Sec. 100 *et seq*. While our individual groups may have other suggestions or concerns, we jointly make the following suggestions. We look forward to working with you to protect the privacy rights of Californians. Thank you for considering our proposals.

[1] *See* Initiative 19-0021, *California Privacy Rights and Enforcement Act of 2020* (Oct. 9, 2010), https://www.oag.ca.gov/initiatives/active-measures.

Sec. 100(a)(1): Notice of new collection and use of personal information

CCPA provides that a business "shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice …" Sec. 100(a)(1). This is an important way to ensure that a business thinks twice before collecting new information and/or using old information in new ways. It also is an important way to ensure that businesses inform consumers about new collection and use of information.

Unfortunately, CPREA would weaken this important CCPA notice rule by limiting it just to new collections and uses "that are incompatible with the disclosed purpose for which the personal information was collected." This would place businesses in the position of deciding whether a new purpose was "compatible" with disclosed purposes, undermining this transparency provision of CCPA.

Thus, the coalition proposes the following changes to the second sentence of CPREA Sec. 100(a)(1):

> A business shall not collect additional categories of personal information or use personal information collected for additional purposes ~~***that are incompatible with the disclosed purpose for which the personal information was collected, or other subsequently disclosed purposes,***~~ without providing the consumer with notice consistent with this section.

Sec. 100(a)(2): Notice of new collection and use of sensitive personal information

CPREA would add a new notice rule as to "sensitive personal information." Sec. 100(a)(2). This new notice rule contains the same flawed "incompatible with disclosed purpose" language just discussed above. The coalition again suggests removing this language as described above.

Sec. 100(c): Minimization

CPREA would add language on "minimization," that is, a requirement that companies minimize their processing of personal information. We request two improvements. First, minimization should extend not just to collection, but also to use, retention, and sharing. Second, minimization should not be pegged to the business' purpose, which may be unclear to the consumer, and may be unilaterally changed by the business. Rather, minimization should be pegged to the customers' reasonable expectations. These improvements to minimization would advance transparency and limit unwanted business processing of personal information, while still subject to all of CCPA's exceptions.

Thus, the coalition proposes the following changes to CPREA Sec. 100(c):

> A business's collection***, use, retention, and sharing*** of a consumer's personal information shall be limited to personal information that is reasonably necessary ***to***

> ***provide a service or conduct an activity that a consumer has requested*** ~~to achieve the purposes for which it is collected~~.

Sec. 100(e): Accuracy

CPREA would add the following accuracy requirement: "A business that collects a consumer's personal information shall take reasonable steps in light of the nature of the personal information and the purposes of processing the personal information to ensure that it does not collect, retain, or share inaccurate personal information." Sec. 100(e).

It is helpful to amend CCPA to ensure that inaccurate information does not harm consumers. But the proposed CPREA language does not tailor a business' duty to ensure accuracy to prevention of harm to consumers. This is a problem, because the pursuit of accuracy for its own sake could lead businesses to gather even more information about consumers, which would harm privacy. Moreover, requiring accuracy without considering the potential harms poses risks to people's privacy and safety.[2] A good model to approach this issue is the federal Privacy Act, 5 U.S.C. 552a(e)(5).

Thus, the coalition proposes deletion of CPREA Sec. 100(e) and substitution of the following:

> A business shall maintain all personal information which it uses to make determinations about any consumer, or shares with another business that will use it to make determinations about any consumer, with such accuracy, relevance, and timeliness as is reasonably necessary to assure fairness to the consumer in the determination.

Secs. 100(h) & 130(d): Trade secrets exemption from disclosure

CPREA would add: "Nothing in this section shall require a business to disclose trade secrets, as specified in regulations …" Secs. 100(h) & 130(d).

CCPA already empowers the California Attorney General to promulgate any necessary exemptions for trade secrets. Sec. 185(a)(3). Any trade secrets issues are better sorted through the existing regulatory process, as opposed to the initiative process. Moreover, many businesses overbroadly interpret the concept of "trade secrets."

Thus, the coalition proposes removal of CPREA Secs. 100(h) and 130(d).

Sec. 105(c)(3): Deletion requests made by consumers directly to service providers

CPREA would empower service providers or contractors to refuse to comply with a deletion request submitted by the consumer directly to the service provider or contractor. Sec 105(c)(3). In such cases, the service provider or contractor should be required to direct the consumer to the business where the consumer should instead make their deletion request.

[2] Lil Miss Hot Mess, *Facebook's "real name" policy hurts real people and creates a new digital divide*, The Guardian (June 3, 2015), https://www.theguardian.com/commentisfree/2015/jun/03/facebook-real-name-policy-hurts-people-creates-new-digital-divide.

Thus, the coalition proposes the following changes to CPREA Sec. 105(c)(3):

> A service provider or contractor shall cooperate with the business in responding to a verifiable consumer request, and at the direction of the business, shall delete personal information about the consumer collected, used, processed, or retained by the service provider of the contractor on behalf of the business. ~~, but~~ ***A service provider or contractor*** shall not be required to comply with a deletion request submitted by the consumer directly to the service provider or contractor to the extent that the service provider or contractor has collected, used, processed, or retained the consumer's personal information in its role as a service provider or contractor. ***In such cases, the service provider or contractor shall direct the consumer to the business where the consumer can submit their deletion request.*** The service provider or contractor shall direct any service providers, contractors or third parties who may have accessed ~~such~~ personal information from or through the service provider or contractor to delete the consumer's personal information.

Sec. 105(d)(1): Deletion exemption for anticipated actions

CPREA would add an exemption from deletion requests for "actions reasonably anticipated by the consumer." Sec. 105(d)(1). Arguably, consumers may reasonably anticipate that businesses will collect, use, and share their personal information for purposes of behavior tracking to display targeted advertising. If so, this would improperly create an adtech exemption from the right to delete.

Thus, the coalition proposes the following changes to CPREA Sec. 105(d)(1):

> Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, ***or*** **~~perform actions~~** reasonably anticipated by the consumer within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

Sec. 105(d)(2): Deletion exemption for "security and integrity"

CCPA has an exemption from the right-to-delete as needed by a business to "detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity." Sec. 105(d)(2). This may already be too broad, as many businesses purport to detect fraud by collecting, maintaining, using, and sharing massive quantities of personal information.

CPREA would dramatically expand this exemption. It does so by defining a new term, "security and integrity," which includes the above anti-fraud language, and adds "the ability of … a network or an information system to function operationally as designed and to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information." Sec. 140(ac). This new language apparently would include adtech, which is an "information system" that is "designed" for behavior-tracking.

Moreover, CPREA would apply this exemption whenever necessary to "help to ensure" this overbroadly defined "security and integrity." Sec. 105(d)(2). Many business activities only remotely connected to anti-fraud efforts will arguably "help to ensure" such efforts.

Thus, the coalition proposes the removal of all changes made by CPREA Sec. 105(d)(2) and reversion to the original CCPA language.

Sec. 105(d)(9): Duplicative deletion exemption for "compatible" internal uses

CCPA has two deletion exemptions for internal use, one for uses "reasonably aligned with expectations of the consumer based on the consumer's relationship with the business," and one for using information "in a lawful manner that is compatible with the context in which the consumer provided the information." Sec. 105(d)(7) and (9), respectively. The second exemption is duplicative of the first, and to the extent it permits additional uses beyond a consumer's expectations based on an ongoing business relationship, it is overbroad.

Thus, the coalition proposes deletion of CCPA Sec. 105(d)(9).

Sec. 110(a)(4) & (c)(4): Right-to-know about specific recipients

Current CCPA provides a right-to-know "the categories of third parties with whom the business shares personal information," but not the specific third parties. Secs. 110(a)(4) & (c)(4). This is an important gap: a consumer cannot fully understand how businesses are harvesting and monetizing their personal information, without being able to follow its movement to specific businesses. CPREA does not fill this CCPA gap. It should.

Thus, the coalition proposes the following changes to CCPA Secs. 110(a)(4) and (c)(4):

> The categories of third parties ***and the specific third parties*** with whom the business shares personal information.

Sec. 110(b): Exemption from right-to-know for information in a privacy policy

A key protection of CCPA is the consumer's right-to-know what information a business has collected about them. A new exemption in CPREA would weaken the right-to-know. The new exemption appears to contain a drafting error, so the scope of the new exemption unclear. The intent seems to be to empower a business to refuse to respond to a right-to-know request if the business determines it has already published similar information online; the coalition opposes such a change.

Specifically, current CCPA Sec. 110(b) provides that a business shall disclose information to consumers, pursuant to CCPA Sec. 130(a)(3), which concerns the right-to-know. CPREA would add that a business "shall be deemed to be in compliance" with CPRA Sec. (a)(1)-(5) to the extent information responsive to those sections "is not materially different" than information it has disclosed under Sec. (c)(1)-(5).

But CCPA Sec. 130(c) has no sub-parts (1)-(5), and CCPA Sec. 130(a)(1)-(5) covers both individualized right-to-know responses and generalized online privacy policies. So there seems to be a scrivener's error here.

Perhaps the intention of this CPREA section is: if a business has published an online privacy policy, and if information responsive to an individualized right-to-know request would not be "materially different" than the published information, then a business may refrain from responding to the right-to-know request. The coalition would oppose such a change. This nebulous standard ("not materially different") gives too much discretion to businesses. Also, even when this standard it met, the business should be required to inform requesters on an individualized basis that the information they seek is located in the online privacy policy.

Thus, the coalition proposes the removal of all changes made by CPREA Sec. 110(b) and reversion to the original CCPA language.

Sec. 120(c): Right to opt-out of advertising

CPREA would allow consumers to opt-out of the use of their "sensitive personal information" for advertising and marketing, and from the disclosure of this information for this purpose to a service provider or contractor. Sec. 120(c). *See also* Sec. 140(ae) (defining "sensitive personal information"). This new rule would not limit the use and disclosure of what CPREA deems to be non-sensitive personal information for the same purposes.

This new rule should be extended to *all* personal information. A great deal of personal information that CPREA deems non-sensitive raises extraordinary privacy concerns, including immigration status, political party registration, telephone and email metadata (*i.e.*, who called whom and when), education attainment, job history, and familial relationships. Surveillance-based adtech is one of the greatest menaces to consumer data privacy. Consumers should be able to opt-out of businesses using *any* of their personal information for advertising and marketing.

Thus, the coalition proposes the following changes to CPREA Sec. 120(c):

> A consumer shall have the right, at any time, to direct a business that uses or discloses **~~sensitive~~** personal information about the consumer for advertising and marketing not to use the consumer's **~~sensitive~~** personal information, or disclose it to a service provider or contractor, for advertising and marketing. A business that uses or discloses a consumer's **~~sensitive~~** personal information for advertising and marketing shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be used, or disclosed to a service provider or contractor, for advertising and marketing and that consumers have the "right to opt-out" of the use or disclosure of their **~~sensitive~~** personal information for advertising and marketing.

Sec. 125: No retaliation for exercise of CCPA rights

If a consumer exercises one of their CCPA rights, CCPA generally prohibits a business from discriminating against them by charging a higher price or providing a lower quality. Sec. 125(a)(1). Unfortunately, CCPA contains a broad exception from this rule, for price and quality differences that are directly related to the value of the consumers' personal information. Sec. 125(a)(2) & (b). The coalition opposes such "pay for privacy" schemes, and their allowance by CCPA. These schemes discourage all consumers from exercising their CCPA rights. They will lead to privacy "haves" and "have nots," because some people cannot afford to pay for their privacy. And they violate the fundamental human right to privacy guaranteed by the California Constitution.

Thus, the coalition proposes the deletion of CCPA Sec. 125(a)(2) & (b).

Sec. 130(a)(2)(B): Limit on period of time covered by access requests

CCPA limits access requests to the 12-month period preceding the request. Sec. 130(a)(2)(A). CPREA would allow a consumer to request access to personal information from a lengthier period of time. Sec. 130(a)(2)(B). However, CPREA places this limit on such requests for more than a year of information: "unless doing so would involve a disproportionate amount of information or would be unduly burdensome." Sec. 130)(a)(2)(B). This standard is vague and does not assign a burden of proof. A better approach is set forth in CCPA Sec. 145(e)(3), which allows a business to refuse to respond to a consumer request, or charge a reasonable fee to do so, if the business can prove the request is "manifestly unfounded or excessive."

Thus, the coalition proposes the following changes to the first sentence of CPREA Sec. 130(a)(2)(B):

> The disclosure of the required information shall cover the 12-month period preceding the business's receipt of the verifiable consumer request, provided that, upon the adoption of a regulation pursuant to paragraph (9) of subdivision (a) of Section1798.185, a consumer may request that the business disclose the required information beyond the 12-month period and the business shall be required to provide such information unless ***the business can prove that the request is manifestly unfounded or excessive*** ~~doing so would involve a disproportionate amount of information or would be unduly burdensome~~.

Sec. 130(a)(3)(B)(iii): Exception to portability

CPREA provides the consumer a right to access specific pieces of personal information in a "portable" form that, if technically feasible, is in a "structured, commonly used, machine-readable format." Sec. 130(a)(3)(B)(iii). But CPREA then exempts information generated "to help ensure security and integrity." *Id.* As discussed above, CPREA's definition of "security and integrity" is vague and overbroad. *See* Sec. 105(d)(2).

Thus, the coalition proposes the following changes to CPREA Sec. 130(a)(3)(B)(iii):

> Provide the specific pieces of personal information to the consumer in a portable and, to the extent technically feasible, structured, commonly used, machine-readable format that is easily understandable to the average consumer and transmit this information to another entity at the consumer's request without hindrance. ~~"Specific pieces of information" do not include data generated to help ensure security and integrity or as prescribed by regulation.~~

Sec. 130(5)(C): Limit on right-to-know about profiling

CPREA would create a new right-to-know whether a company is "profiling" consumers and using their personal information to determine their eligibility for loans, housing, insurance, education, employment, or health services. Sec. 110(c)(6). CPREA defines "profiling" as automated processing of personal information to make predictions about a consumer's work performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. Sec. 140(z).

Unfortunately, CPREA then limits this right-to-know about profiling just to circumstances in which "such profiling had, or could have reasonably been expected to have, a significant, adverse effect on consumers." Sec. 130(5)(C). This limit should be removed. A consumer should be allowed to ascertain whether a business' profiling helped them get a job, or had a less-than-significant adverse effect on their ability to get a loan.

Thus, the coalition proposes the following changes to the first sentence of Sec. 130(5)(C):

> For purposes of paragraph (6) of subdivision (c) of Section 1798.110, disclose whether the business uses consumers' personal information for profiling~~, if such profiling had, or could have reasonably been expected to have, a significant, adverse effect on consumers~~ with respect to: (i) financial lending and loans; (ii) insurance; (iii) health care services; (iv) housing; (v) education admissions; or (vi) denial of employment.

Sec. 140(a): Definition of "advertising and marketing"

CPREA creates a right to opt-out of "advertising and marketing" that uses sensitive personal information. Sec. 120(c), 120(g), 135. Unfortunately, CPREA narrowly defines "advertising and marketing" as just communications intended to induce a consumer to pay for a good or service. This does not capture business advertising intended to build consumer goodwill for the business, such as a description of a business' charitable work. Nor does it capture business advertising on public policy questions, such as encouragement of consumers to tell their elected officials to oppose a bill that might hurt the business.

Thus, the coalition proposes the following changes to CPREA Sec. 140(a):

> "Advertising and marketing" means a communication by a business or a person acting on the business's behalf in any medium intended***: (1)*** to induce a consumer to buy, rent, lease, join, use, subscribe to, apply for, provide, or exchange products, goods, property,

> information, services, or employment***; (2) to make it more likely that a consumer will take an action based on the communication; or (3) for a business or commercial purpose.***

Sec. 140(e)(2): Security component of the definition of "business purpose"

CCPA provides a right to opt-out of the sale of personal information. Sec. 120. The definition of "sale" limits this right by excluding various business activities from this term. Sec. 140(ad). Most relevant for current purposes, the definition of "sale" excludes a business' transfer of personal information to a service provider for "a business purpose." Sec. 140(ad)(2)(C).

CPREA would shrink the right to opt-out of sales by expanding the definition of "business purpose." Sec. 140(e)(2). Specifically, at the security component of business purpose, CPREA would adopt the same vague and overbroad "security and integrity" language discussed above. *See* Sec. 105(d)(2).

Thus, the coalition proposes the removal of all changes made by CPREA Sec.140(e)(2) and reversion to the original CCPA Sec. 140(d)(2) language.

Sec. 140(e)(4): Adtech component of the definition of "business purpose"

CCPA has an adtech component of "business purpose." Sec. 140(e)(4). As just discussed, it limits the right to opt-out of sales of personal information. CPREA would delete the following language from this adtech component: "including, but not limited to, the contextual customization of ads shown as part of the same interaction."

Unfortunately, CPREA then would add this language: "including but not limited to non-personalized advertising shown as part of the consumer's same interaction with the business." Sec. 140(e)(4). CPREA would define "non-personalized advertising" as ads "not based on a consumer's past behavior." Sec. 140(t). This would allow advertising based on other aspects of a consumer's identity.

Thus, the coalition proposes the following changes to CPREA Sec. 140(e)(4):

> Short-term, transient use, ~~including but not limited to non-personalized advertising shown as part of the consumer's same interaction with the business,~~ provided that the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction with the business.

Alternately, the coalition proposes a more privacy-protective definition of "non-personalized advertising." Sec. 140(t). CPREA defines this term as advertising "not based on a consumer's past behavior." This would allow advertising based on any personal information that does not comprise past behavior, such as a consumer's race, city of birth, and parentage. So "non-personalized advertising" should exclude any use of personal information. Specifically, the coalition proposes the following changes to CPREA Sec. 140(t):

> "Non-personalized advertising means advertising and marketing that is not based on a consumer's ***personal information*** ~~past behavior~~.

Sec. 140(k): Definition of "deidentified"

CCPA defines "deidentified" information as information that cannot reasonably "identify, relate to, describe, [be] associated with, or be linked [] to" a "particular consumer." It further provides specific safeguards to prevent subsequent efforts to "reidentify" the information. These safeguards are intended to recognize the reality that deidentification efforts may fail, rather than to suggest that information is "deidentified" even if it can readily be reidentified.

CPREA would amend this language in two detrimental ways. First, it would substitute "identifiable consumer" for "particular consumer" in the core definition. Sec. 140(k). This change could be interpreted to mean that information linked to an identifier such as a cookie ID that is designed to recognize and track particular consumers would qualify as "deidentified" if it could not be used to derive that consumer's name or otherwise render the consumer "identifiable" (which is not a defined term). In addition, the proposed safeguards explicitly authorize a business to reidentify deidentified information, Sec. 140(k)(B), which is inconsistent with the concept of deidentification as an irreversible process.

Thus, the coalition proposes the removal of all changes made by CPREA Sec.140(k) and reversion to the original CCPA Sec. 140(h) language.

Sec. 140(m): Definition of "device"

CCPA defines "personal information" (the core term in all CCPA protections) by reference to "a particular consumer or household." Sec. 140(v)(1). It defines "household," in turn, by reference to a group of consumers living in one residence who share a "device." Sec. 140(p).

CPREA would narrow the definition of "device," which in turn would narrow "household" and then "personal information." Specifically, CPREA would limit "device" to objects capable of connecting to the internet, directly or indirectly, but exclude devices that connect only to other devices. But many powerful technologies, such as RFID chips, can track individuals and collect sensitive information by connecting to other devices without directly or indirectly connecting to the internet. This limitation unduly narrows the scope of personal information. If a device collects personal information and that personal information is held by a business, all the CCPA's privacy rights should apply to that information. The particular path the information took—i.e., over a direct or indirect connection to the Internet, or through another device—is less important than the fact that the business holds a consumer's personal information.

Thus, the coalition proposes the removal of all changes made by CPREA Sec.140(m) and reversion to the original CCPA Sec. 140(j) language.

Sec. 140(p): Definition of "household"

Again, CCPA defines "personal information" in part by reference to "household." Sec. 140(v)(1). CPREA would add a definition of "household." Sec. 140(p). This definition would focus on shared "access" to a device or service, which unfortunately could be interpreted narrowly to mean just the ability to access secure settings with a password. The definition instead should focus on shared "use," *i.e.*, the ability of anyone in the residence to interact with the device. Moreover, this definition is limited to devices and services provided by a business, which excludes devices and services provided by a government agency or non-profit organization. The definition instead should apply to all devices and services.

Thus, the coalition proposes the following changes to CPREA Sec. 140(p):

> "Household" means a group, however identified, of consumers who cohabitate with one another at the same residential address and share ***use of*** ~~access to~~ common device(s) or service(s)~~ provided by a business~~.

Sec. 140(v)(2): Definition of "publicly available"

"Publicly available information" is excluded from the definition of "personal information." Sec. 140(v)(2). As recently amended by A.B. 1355 (Assemblymember Chau), CCPA defines "publicly available" as "information that is lawfully made available from federal, state, or local government records." Sec. 140(o)(2).

CPREA would make two inappropriate changes to this definition of "publicly available." First, it would exclude information "used for a purpose that is not compatible with the purpose for which the data is maintained and made available in government records unless the information is a matter of public concern." This restores a defect that was cured by A.B. 874. Once a person lawfully obtains information from the government, they should be allowed to use it as they see fit, without having to prove their purpose was compatible with the government's purpose, or that the information is a matter of public concern.

Second, CPREA would expand the definition of "publicly available" to include "information that a business has a reasonable basis to believe is lawfully made available to the general public [i] from widely distributed media, or [ii] by the consumer, or [iii] by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience." This would be a massive diminution of the scope of "personal information" and thus of all CCPA protections.

Thus, the coalition proposes the removal of all changes made by CPREA Sec.140(v)(2) and reversion to CCPA Sec. 140(o)(2), as amended by A.B. 1355.

Finally, narrow tailoring is required for any CCPA amendment to address personal information that a consumer intentionally makes available to the general public by means of the internet or similar technologies. Also, any amendment for this purpose should be made to the CCPA's definition of sale, without otherwise changing the scope of personal information. If such an amendment is desired, the coalition proposes the following new exemption from the definition of "sale," as a new subparagraph (D) to CCPA Sec. 140(t)(2):

> The business shares personal information that a consumer intentionally made available to the general public via a channel of mass media, without restriction to a particular audience.

Secs. 140(ag): Definition of "service provider"

Under CCPA, a "service provider" processes information for a business. Sec. 140(ag). Certain CCPA rules do not apply to information transfers between businesses and their service providers. For example, a business does not "sell" information when it transfers it to a service provider for a business purpose, Sec. 140(ad)(2)(C), and so the consumers' right to opt-out of information sales does not extend to such business-to-provider transfers.

CPREA would empower a service provider to combine (i) the personal information they obtain from one business, with (ii) the personal information they obtain from another business, or on their own – so long as the service provider does so for "any business purpose," and in compliance with new California regulations. Sec. 140(ag)(1).[3] This would be a new CCPA loophole for the creation of more comprehensive profiles of consumers based on larger volumes of their personal information.

Thus, the coalition proposes the following changes to CPREA Sec. 140(ag)(1)(C):

> combining the personal information which the service provider receives from or on behalf of the business, with personal information which it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer~~, provided that the service provider may combine personal information to perform any business purpose, except as provided for in paragraph (5) of subdivision (e) of this Section and in regulations adopted by the California Privacy Protection Agency~~.

Sec. 140(ah): Definition of "third party"

CPREA would expand the definition of "third party" to include "a service provider to the business" and "a contractor." Sec. 140(ah)(2) & (3). This suggest that any contractor qualifies as a third party, not merely a contractor to the business.

Thus, the coalition proposes the following changes to CPREA Sec. 140(ah)(3):

> A contractor ***to the business***.

[3] This CPREA section would also bar such combining "as provided by in paragraph (5) of subdivision (e) of this Section," but it is not clear what subdivision this refers to.

Sec. 140(aj): Definition of "verifiable consumer request"

A critical issue undergirding all CCPA rights is "verification," that is, proof by the requester to the business that they are actually the consumer described in the personal information at issue. This requires careful balancing of the need for straightforward consumer exercise of their CCPA rights, with prevention of adversaries unlawfully obtaining access to, or destruction of, a consumer's personal information. CCPA properly requires the California Attorney General's Office to promulgate regulations on this issue. Sec. 185(a)(7). That Office recently published draft regulations that address this issue. Also, recently-enacted A.B. 1355 contains further refinements of the verification process. Such administrative and legislative measures have the flexibility needed to address the complex issues surrounding verification. *See* Amended Sec. 130(a)(2).

At this juncture, it is not helpful to revise the verification process by means of an initiative. *See* Sec. 140(aj). Initiatives are harder to change than other ordinary laws, yet this issue requires flexibility. Further, it is counterproductive to require "commercially reasonable methods" of verification, as this term is undefined, and arguably invites a business to consider its own commercial interests to an excessive degree.

Thus, the coalition proposes the removal of all changes made by the first sentence of CPREA Sec. 140(aj).

Sec. 145(a)(1): Exemption for compliance with law

CCPA exempts actions taken to "comply with federal, state, or local laws." Sec. 145(a)(1). CPREA would unduly expand this already-overbroad exemption. First, CPREA would extend the exemption to "applicable" laws, which apparently would include unspecified laws beyond those of the federal, state, and local governments. Second, it would expand this exemption to "valid legal process," which is undefined, and would arguably include all manner of government requests outside the bounds of judicial oversight. Third, it would extend to business disclosure of information "as otherwise required by law." While this new language seems redundant of the original language, a court applying the "no surplusage" protocol of statutory interpretation might take it to mean something new.

Thus, the coalition proposes the removal of all changes made by CPREA Sec. 145(a)(1) and reversion to the original CCPA language.

Sec. 145(a)(2): Exemption for investigation

CCPA allows a business to "[c]omply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities." Sec. 145(a)(2). Such access demands often are based just on an investigator's say-so, without any judicial supervision. Given the inherent privacy invasion when police seize personal information about a customer from a business, CPREA should amend CCPA to require judicial supervision of such seizures. *Cf.* Cal. Penal Code 1546.1 (requiring a court order for government access to electronic communications and electronic device information held by a business about a consumer).

Thus, the coalition proposes deletion of the first sentence of CPREA Sec. 145(a)(2), and substitution of the following:

> Comply with a court-issued subpoena, order, or warrant.

Sec. 145(a)(2): Preservation orders from police

CPREA would empower police to "direct a business not to delete a consumer's personal information, pending a court order or other legal process." Sec. 145(a)(2). Such new power for police to order a business to preserve a consumer's information would be a substantial intrusion on the prerogative of consumers to control their information, including to delete it if they wish.

Thus, the coalition proposes deletion of the second sentence of CPREA Sec. 145(a)(2).

It may be possible to write a properly tailored CCPA provision on preservation orders. Such a provisions would need many privacy safeguards the CPREA lacks. For example, such a provision would need a time limit. *See, e.g.,* 18 U.S.C. 2703(f)(2) (placing a 90-day limit on preservation orders). If police cannot obtain the necessary access order from a court by the deadline, then the consumer must regain their right to delete. Also, such a provision would need prompt notice to the consumer. *See, e.g.,* Cal. Penal Code 1546.2 (requiring notice to consumers of the seizure of their electronic information). Such notice is necessary to give consumers the opportunity to go to court to challenge the preservation order. In any event, drafting such a provision on preservation orders is best left to the ordinary legislative process.

Sec. 145(a)(4): Exemption for child welfare

CPREA would create a massive new CCPA exemption for businesses to "[r]espond to requests by government agencies for personal information that is necessary to carry out child welfare, foster care, adoption, or parental support programs …" Sec. 145(a)(4). This would empower a business to freely collect any personal information they wish, and then sell it to the government, if that personal information is arguably pertinent to the government's many "child welfare" programs.

This proposal lacks merit for many reasons. First, because businesses do not know who might someday be involved in the child welfare system, they will have every incentive to collect personal information about everyone (free from all CCPA limits), in order to have a useful dataset they can sell to child welfare officers. Second, because of the substantial racial disparities that have long plagued the child welfare system,[4] the application of these unregulated databases may cause further racial disparity. Third, during the 2019 legislative session, the California Legislature rejected A.B. 1416, which like this CPREA proposal would have authorized businesses to ignore CCPA when they amass personal information for purposes of subsequent sale to government.

[4] *See, e.g.,* National Conference of State Legislatures, *Disproportionality and Disparity in Child Welfare* (Aug. 1, 2017), http://www.ncsl.org/research/human-services/disproportionality-and-disparity-in-child-welfare.aspx.

Thus, the coalition proposes deletion of CPREA Sec. 145(a)(4).

Sec. 145(a)(5): Exemption for emergency

CPREA would create a new exemption for a business to "[c]ooperate with government agencies if the business believes in good faith that the consumer is at risk of danger of death or serious physical injury and the situation requires disclosure of the consumer's personal information without delay." Sec. 145(a)(5).

As written, CPREA lacks many of the privacy safeguards needed to ensure that an emergency exception does not swallow the rule. First, the agency at issue should only be allowed to request emergency access to information with the approval of a high-ranking agency officer. *See, e.g.,* 18 U.S.C. Sec. 2518(7). Second, that agency officer must be required to have good faith grounds to believe that they would have a lawful basis to obtain the information on a non-emergency basis. *See, e.g., id.* at 2518(7)(b). Third, the agency must be required, within three days, to petition a court for the appropriate order, and if that order is not granted, the agency must be required to immediately destroy all information that it obtained on an emergency basis. *See, e.g.,* Cal. Penal Code Sec. 1546.1(h). Fourth, the agency must be required to promptly notify the person whose information was seized. *Id.* at Sec. 1546.2(a).

Thus, the coalition proposes deletion of CPREA Sec. 145(a)(5).

It may be possible to write a properly tailored CCPA exemption for business cooperation with police in an emergency. But such drafting is best left to the ordinary legislative process.

Secs. 145(j) & 145(k): Exemptions for employees

During the 2019 legislative session, there was substantial discussion about whether to create a CCPA exemption for employees, and if so, how to scope that exemption. Participants included legislators, businesses, employee advocates, and privacy advocates. The stakeholders agreed to spend the 2020 legislative session attempting to forge compromise on this issue. Towards that end, A.B. 25 (Chau) created a one-year delay on the application of CCPA to employees, by means of a one-year exemption for employees that sunsets on January 1, 2021. Sec 145(g)(2) & 145(m)(2). CPREA would disrupt this attempt to forge compromise, by creating permanent exemptions for employees that have no sunsets. Secs. 145(j) & 145(k).

Thus, the coalition proposes deletion of CPREA Secs. 145(j) & (k).

Sec. 145(l): Exemption for commercial credit reporting

CPREA would exempt processing by commercial credit reporting agencies of "business controller information" (*i.e.*, the names and contact information of those controllers) used solely to identify the relationship of a consumer to a business they own, or to contact the consumer as the owner of the business. Sec. 145(l). However, no other privacy law applies to the processing of this personal information, so this exemption would create a gap in protection. Also, business owners should be able to exercise their rights to delete and to opt-out of sales.

Thus, the coalition proposes deletion of CPREA Sec. 145(l).

Sec. 145(m): Exemption for households

CPREA would exempt household data from the CCPA right to delete, some of the CCPA rights to access, and the proposed CPREA right to correct. Sec. 145(m). However, businesses often track personal information by household and not by individual person, in which case CCPA rights must be exercised by households in order to be effective. Any concerns about the privacy rights of non-requesting household members should be resolved with precision in a regulatory or legislative process, and not overbroadly in an initiative process.

Thus, the coalition proposes deletion of CPREA Sec. 145(m).

Sec. 145(o): Exemption for yearbooks

The CPREA would exempt, from CCPA rights to delete and to opt-out of the sale of information, a business' use or sale of personal information:

> if [i] the consumer has affirmatively consented to the business's use, disclosure, or sale of the consumer's personal information and [ii] the business has incurred significant expense in reliance on the consumer's affirmative consent, including but not limited to, by producing a physical item such as a school yearbook containing the consumer's photograph, and [iii] compliance with the consumer's request to opt-out of the sale of the consumer's personal information or to delete the consumer's personal information would not be commercially reasonable, [iv] provided that business complies with the consumer's request as soon as it is commercially reasonable to do so.

Sec. 145(o) (bracketed numbers added).

Any exemption of this nature must be far narrower. First, it must account for the strong privacy interest that consumers have in withdrawing consent to process their information. Second, it must distinguish between physical items that contain personal information, which are harder for a business to modify, and online analogs, which are much easier for a business to modify. Third, the scope of the exemption must be tailored to the scope of the consent.

Thus, the coalition proposes the following changes to CPREA Sec. 145(o):

> Sections 1798.105 and 1798.120 shall not apply to a business's use, disclosure, or sale of ***particular pieces of*** a consumer's personal information if the consumer has affirmatively consented to the business's use, disclosure, or sale of ~~the consumer's personal~~ ***that*** information ~~and the business has incurred significant expense in reliance on the consumer's affirmative consent, including but not limited to, by producing~~ ***to produce*** a physical item, such as a school yearbook containing the consumer's photograph, ***if:***

> ***(1) The business has incurred significant expense in reliance on the consumer's affirmative consent;***
>
> ***(2)*** ~~and c~~***C***ompliance with the consumer's request to opt-out of the sale of the consumer's personal information or to delete the consumer's personal information would not be commercially reasonable***; and***
>
> ***(3)*** ~~, provided that~~ ***The*** business complies with the consumer's request as soon as it is commercially reasonable to do so.

Sec. 150: Private right of action

CCPA provides a private right of action, but only to challenge certain data breaches. Sec. 150. But a statutory right is only as strong as its enforcement, and the best form of enforcement is a private right of action. All too often, government agencies with a duty to enforce a statute will lack the resources to effectively do so, or suffer "regulatory capture." A private right of action must include the remedy of attorney fees (to ensure access to the courts), and not be subject to a business' right to cure (which unduly blocks enforcement).

Thus, the coalition proposes that replacing the language of CPREA Sec. 150 with the following:

> (a) Any violation of this Act constitutes an injury in fact, and any consumer may bring a lawsuit in a court of competent jurisdiction.
>
> (b) Any consumer whose personal information is subject to an unauthorized access and exfiltration, theft, or disclosure may bring a lawsuit in a court of competent jurisdiction.
>
> (c) A consumer who prevails in such a lawsuit shall obtain the following remedies:
>
> > (1) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty dollars ($750) per consumer per incident or actual damages, whichever is greater.
> >
> > (2) Injunctive or declaratory relief.
> >
> > (3) Reasonable attorney fees and costs.
> >
> > (4) Any other relief the court deems proper.

Sec. 155: Agency enforcement

CCPA provides for enforcement of CCPA by state government. Sec. 155. So would the CPREA (though it would change which unit of state government). Sec. 155. However, effective enforcement requires a greater diffusion of enforcement authority. County District Attorneys, City Attorneys, and Corporation Counsels are also well-positioned to enforce the law. They should be permitted to do so and to contract with private attorneys to facilitate that enforcement.

Thus, the coalition proposes deletion of CPREA Sec. 155(a), and substitution of the following:

> The California Attorney General, the California Privacy Protection Agency, a county district attorney, a city attorney, or a county counsel may bring a civil action, in the name of the people of the State of California, against any business, service provider, or other person that violated this title. These units of government may contract with private attorneys to facilitate this enforcement.

Sec. 180: Preemption of local laws

CCPA preempts all laws adopted by county or local agencies regarding business collection and sale of consumer personal information. Sec. 180. This deprives California residents of the opportunity to petition their local and county governments for laws to protect their data privacy that are even more privacy-protective than CCPA. It also deprives state government of the opportunity to learn from the experiences of local government with new policy approaches to evolving technological challenges to consumer data privacy.

Thus, the coalition proposes the deletion of CPREA Sec. 180.

Sec. 185(a)(10): Regulations on combining data sets

CPREA requires the creation of regulations governing when a service provider may combine data sets. Sec. 185(a)(10). As discussed above, the coalition proposes the removal from CPREA of authorization to service providers to combine the data sets they obtain from different businesses. *See* Sec. 140(ag)(1). We likewise propose removal of CPREA language requiring new regulations governing when a service provider may combine data sets. Sec. 185(a)(1). Service providers should never be authorized to combine data sets, so no regulations are needed.

Thus, the coalition proposes the deletion of CPREA Sec. 185(a)(10).

Sec. 185(d): Timeline for regulations

CPREA establishes a new deadline for adoption of regulations (January 1, 2022). Sec. 185(d). It is not clear whether this new deadline extends narrowly to just the new CPREA language, or more broadly to the old CCPA language. It is important to be clear that CPREA would not affect CCPA's deadlines for CCPA regulations, implementation, and enforcement.

Thus, the coalition proposes the following changes to CPREA Sec. 185(d):

> Notwithstanding subdivision (a), the timeline for adopting final regulations ***newly*** required by the ***California Privacy Rights and Enforcement Act of 2020*** ~~Act adding this subdivision~~ shall be January 1, 2022.

Sec. 30: Operative date

CPREA provides that its terms "only apply to personal information collected by a business on or after January 1, 2020." But consumers should have the rights to access, delete, correct, and block the sale of earlier-collected personal information.

Thus, the coalition proposes the following changes to CPREA Sec. 30:

> This Act shall become operative on January 1, 2021 ~~and shall only apply to personal information collected by a business on or after January 1, 2020~~.

* * *

We thank you for your work to advance consumer data privacy in California, and for your consideration of the above ways to strengthen CPREA and CCPA. We hope we can meet with you soon to discuss our suggestions. If you have any questions, please do not hesitate to reach out to Sam Corbin (samantha@corbinandkaiser.com) or Kevin Baker (kbaker@acluca.org).

Sincerely,

American Civil Liberties Union of California
CALPIRG
Center for Digital Democracy
Common Sense Media
Consumer Action
Consumer Federation of America
Consumer Reports
Electronic Frontier Foundation
Media Alliance
Oakland Privacy
Privacy Rights Clearinghouse