November 8, 2021

California Privacy Protection Agency
Attn: Debra Castanon
915 Capitol Mall, Suite 350A
Sacramento, CA 95814

Subject: PRO 01-21

To the California Privacy Protection Agency,

We are a coalition of civil society, privacy and consumer advocacy organizations working in California dedicated to improving privacy protections, and we appreciate the California Privacy Protection Agency ("the Agency") invitation to comment on the proposed rulemaking under the California Privacy Rights Act of 2020 ("CPRA").

We respectfully ask that the Agency ensure implementing CPRA regulations do not erode California Consumer Privacy Act ("CCPA") protections, and recommend the Agency require businesses to include a "Do Not Sell My Personal Information" link on the business's webpage *and* honor a consumer's privacy choice exercised through a browser signal, setting or plug-in. Additionally, we encourage the Agency to craft regulations that give consumers easy ways to exercise their rights in every context and on every device. To that end, we ask the Agency to require businesses to respect existing, widely-deployed privacy settings and signals on multiple platforms, and to interpret those signals in accordance with consumer intent rather than requiring signals to be specifically tailored to the language of CPRA.

Global privacy settings have the obvious benefits to consumers of being simple to understand and easy to enable, and we believe that regulations which foster the adoption of such controls will help CPRA deliver on its intent. However, the ways that businesses interpret privacy settings may not always be clear or intuitive to consumers. For example, a consumer who has enabled a privacy setting in their browser may believe that they have opted out of sale with respect to every business they interact with on the Web, when, in fact, not every business will be able to associate that signal with the consumer's identity on other platforms. We request that the Agency give consumers ways to know whether, and to what extent, their privacy settings are respected.

**Implementing regulations should continue to require businesses to include a "Do Not Sell My Personal Information" link and treat user-enabled global privacy controls as valid Requests to opt out**

Current CCPA regulations require businesses to treat user-enabled global privacy controls, such browser plug-ins or privacy settings, as valid requests to opt out of the sale of information to third parties.[1] Critically, this is independent of the requirement that businesses include a prominently placed link on their webpage that reads, "Do Not Sell My Personal Information" so that consumers may easily exercise their privacy choices.[2] While the CPRA could be read to make this protective requirement optional[3] we strongly recommend preserving both mechanisms for consumers to opt out. Allowing companies to decide which consumer choices to honor would, in addition to directly contravening the Findings and Declarations, and Purposes and Intent of the CPRA,[4] negatively impact consumer privacy protections and reduce the effectiveness of the CCPA.

The existence of the "Do Not Sell My Personal Information" link conveys to a concerned consumer – and to watchdog organizations like the undersigned – essential information regarding a business's privacy practices and its likely level of compliance with the CCPA. Put simply, both consumers and watchdogs can tell, merely by looking for a "Do Not Sell My Personal Information" Link, whether a company sells consumers' personal information under the law. This at-a-glance information helps inform consumer choices *and* enforcement actions. Indeed, the existence or absence of the link is one of the most easily auditable requirements of the CCPA. The office of the Attorney General, recognizing the value of such a clear indicator of compliance, developed the Consumer Privacy Interactive Tool to allow consumers to easily report obviously non-compliant businesses.[5] Among the 27 CCPA enforcement actions the Office of the Attorney General has spoken about publicly, nearly 30% (8 of the 27) included violations of the requirement to include a "Do Not Sell My Personal Information" link.[6]

The CCPA requires consumers exercise their rights individually on a business-by-business basis – an onerous task made only somewhat less burdensome by the "Do Not Sell My Personal Information" link and the acceptance of user-enabled global privacy controls.

---

[1] 11 CA ADC § 999.315

[2] Civil Code § 1798.135(a)(1), and 11 CA ADC § 999.306(b)(1)

[3] Civil Code § 1798.135(b)(1)

[4] "Rather than diluting privacy rights, California should strengthen them over time." The California Consumer Privacy Act of 2018, A.B. 375, §2(E);
"Consumers need stronger laws to place them on a more equal footing when negotiating with businesses in order to protect their rights" *Id. At* §2(H);
"The rights of consumers and the responsibilities of businesses should be implemented with the goal of strengthening consumer privacy" *Id. At* §3(C)(1)
"The law should be amended, if necessary, to improve its operation, provided that the amendments do not compromise or weaken consumer privacy" *Id. At* §3(C)(6)

[5] Consumer Privacy Interactive Tool, https://oag.ca.gov/consumer-privacy-tool (last visited Nov. 8, 2021)

[6] CCPA Enforcement Case Examples, https://www.oag.ca.gov/privacy/ccpa/enforcement (last visited Nov. 8, 2021)

Unsurprisingly, research suggests that consumers are already having difficulty exercising their privacy choices under the CCPA. A Consumer Reports study in 2020 attempted to act as an intermediary between 124 consumers in California and 21 large companies that deal in personal information – and found barriers to exercising those choices with almost all 21 companies.[7] As part of reporting on the study, Consumer Reports spoke to Joshua Browder, founder of DoNotPay, a company that has been trying to act as an authorized agent for Californians exercising CCPA rights. According to Joshua, "It's been a huge challenge. . . Every day it's like an arms race."[8] The CCPA's requirement that large businesses share annual metrics about consumer requests received, denied and complied with (in whole and in part)[9] further illustrates that consumers are, for the most part, unaware of their CCPA rights. Equifax, one of the largest data brokers in the country, which *exposed* the information of 150 million Americans in 2017, reported that only 623 consumers exercised their Right to Know, and 1,205 consumers exercised their Right to Opt Out in 2020 (an estimated 0.0000015% of the total 800 million users that the business collects and aggregates).[10]

Consumers, in other words, need more help. The Agency should therefore ensure that implementing the CPRA does not result in a rejection of the intent and purposes of the proposition: to strengthen privacy protections for Californians and set a protective floor which cannot be eroded. Allowing a business to omit a "Do Not Sell My Personal Information" link would do just that, resulting in CCPA opt-out options and other notices of privacy choices being buried in a website's privacy policy. It could also hamstring enforcement actions, leaving the Agency unable to rely on watchdog organizations and consumer alerts made through the Consumer Privacy Interactive Tool. Allowing a business to refuse a consumer's opt-out request made through a user-enabled global privacy control would erect yet another barrier to consumers exercising their privacy rights. As the rest of the country looks on, the California Privacy Protection Agency's first actions as enforcement authority should *not* include substantially weakening Californians' existing privacy protections.

**The Agency should require businesses to comply with clear, widely deployed opt-out controls.**

In order to make opt-out signals as useful as possible to consumers, businesses should be required to comply with opt-out technologies that are easy to use and widely deployed. Regulations should account for the different contexts in which consumers interact with businesses.

---

[7] Kaveh Waddell, *Why It's Tough to Get Help Opting Out of Data Sharing*, Consumer Reports, (March 16, 2021) https://www.consumerreports.org/privacy/why-its-tough-to-get-help-opting-out-of-data-sharing-a7758781076/

[8] *Id.*

[9] 11 CA ADC § 999.317(g)

[10] California Residents Privacy Statement and Notice at Collection, https://www.equifax.com/privacy/privacy-statement/#CaliforniaResidents (last visited Nov. 8, 2021)

On the Web, the Global Privacy Control (GPC)[11] is specifically designed to convey a user's intent to opt out of sharing and sale, and it has achieved widespread adoption, including endorsement from the California Attorney General.[12] Technically, it is a simple HTTP header that can be appended to every request that a device makes. It is simple for both client-side software and businesses to implement, and it works whether a user is logged in to a service or interacting with a website anonymously. Businesses should be required to treat a GPC=1 signal coming from a consumer as an opt out of sharing and sale.

Other contexts will require businesses to accept different kinds of opt-out controls. Consumers spend a significant amount of time interacting with mobile phones, often via third-party apps, and the surveillance business model in mobile apps works similarly to the way it does on the Web. Apps collect information about their users, then disclose it to third-party advertisers and data brokers for monetization. However, users enjoy less control over their experience on mobile devices than they do on the Web. Most major web browsers allow users to install "extensions" which customize the way the browser works—for example, by adding a "GPC=1" header to every outgoing request. This allows for rapid development and deployment of novel privacy-preserving tools. But there is no comparable "extension" ecosystem on iOS and Android. For the most part, users can only configure apps in ways that are explicitly allowed by developers of the apps or the operating system itself.

Fortunately, there are existing operating system-level and application-level privacy controls on both iOS and Android. These controls should be considered opt-out requests under CPRA whenever that is practical.

Android has a system-wide preference labeled "Opt out of Ads Personalization," which users can choose to enable in their settings. Apps installed on a user's phone can access that user's opt-out preference with a simple query. This setting is described as follows: "Instruct apps not to use your advertising ID to build profiles or show you personalized ads." Android terms restrict how developers can use other persistent identifiers, like IMEI number, and bar developers from selling personal data at all.[13] Therefore, a consumer choosing to "opt out of ads personalization" is led to believe that the setting will prohibit any sale, or sharing for the purpose of advertising profiling, of their personally-identifiable information. Businesses should respect this signal as a clear opt out of sharing and sale.

Similarly, on iOS, Apple requires apps to ask permission to "track" users before accessing device identifiers, and app store policy prohibits apps from tracking users in other

---

[11] Global Privacy Control (GPC) Unofficial Draft 11 October 2021, https://globalprivacycontrol.github.io/gpc-spec/ (last visited Nov. 8, 2021)

[12] 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/

[13] User Data, Google, https://support.google.com/googleplay/android-developer/answer/10144311?hl=en (last visited Nov. 8, 2021)

ways without receiving such permission.[14] Therefore, a user's refusal to grant an app permission to "track" them should be interpreted as a request to opt out of sharing and sale under CPRA.

**The Agency should not require opt-out signals to be designed specifically for CPRA compliance.**

The Agency should require businesses to comply with any privacy signals that a user reasonably believes to be an expression of their intent to opt out. We continue to oppose the text of the final CCPA regulations at Section 315(d)(1): "Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information." As we've explained, many users already enable privacy controls which convey their desire for protections equivalent to, or stronger than, the opt-out rights granted by CPRA. If the Agency requires each valid opt-out signal to be molded around the exact language present in CPRA, it will lead to a confusing, fractured set of competing technical standards that all convey more-or-less the same thing.

For both the opt out of sharing and sale, and the opt out of use of sensitive personal information, businesses should accept any signal that is widely adopted and that indicates a consumer's desire to exercise rights which are equivalent to, or encompass, their CPRA rights. Businesses should not be able to ignore signals which do not precisely match the language of the statute. For example, a signal which specifies that a user wants to opt out of "tracking" or "profiling" should be interpreted as an expression of their intent to opt out of sharing and sale as well.

Rather than require operating system developers to create new, distinct tools to help users opt out of sharing, sale, and secondary use, the Agency should prefer to encourage businesses to respect existing, widely-deployed privacy controls. Users should not be forced to toggle several different settings on each device they own in order to protect their personal information.

**Regulations should minimize consumer confusion and ensure that businesses process opt-out signals in a transparent way**

We strongly support the inclusion of user-enabled global privacy controls in the CCPA regulations and CPRA ballot initiative. Ensuring that consumers can easily and effectively communicate their privacy choices is enshrined in the intents and purposes of the CPRA. Those purposes rightly stress the importance of consumer control, the ability to opt out of the sale of information to third parties, and specifically references the ability to make privacy choices through authorized agents, as well as browser and device settings and signals.[15] Unfortunately, the current implementation threatens to leave consumers with a mistaken impression of how

[14] App privacy details on the App Store, Apple, https://developer.apple.com/app-store/app-privacy-details/ (Last visited Nov. 8, 2021)

[15] The California Privacy Rights Act of 2020, Proposition 24, §3(A)(2),(4) and §3(B)(1),(4) and §3(C)(1),(3),(4),(5),(6)

effectively they have controlled their personal information – and we encourage the Agency to address this confusion in implementing CPRA regulations.

CCPA regulations require that a business treat user-enabled global privacy controls as an opt-out request for *that device* or, if known, for the consumer submitting the request.[16] For consumers interacting with a business's website without a logged-in experience or a direct connection with the business, user-enabled privacy controls might only apply to the device or browser that consumer was using at the time, and not to the whole body of personal information that the business may possess about the consumer. To be clear, user-enabled privacy controls should **always** be accepted as an opt-out request, and businesses should treat these controls as opt-out requests for the device or browser when the individual consumer is not known. Our concern lies with consumers who may be relying on the belief that a device-level privacy setting has effectively communicated an opt-out request for *all* of their personal information.

Such a consumer would, upon visiting a business's website with a browser setting configured, be given no indication that a GPC signal was received, whether the business honors browser signals, or whether the opt-out request has been interpreted as an opt out for the *device* or for them personally. This consumer, operating under the belief that they have already opted out of the sale of their information to third parties, may not take additional steps to exercise their opt-out rights under the law. They would not know to scour the business's privacy policy for CCPA information or attempt to submit a verified consumer request. This is also a problem for watchdogs trying to hold businesses to account: if a business does not indicate what kind of signals it accepts, or how it processes those signals, it is hard to verify that the business is properly complying with CPRA.

At the very least, businesses should include information in their privacy policies about which privacy settings, controls, and signals they accept, and how those technical opt-out mechanisms are applied. For example, a business which accepts GPC via a website should indicate both how it interprets the GPC signal (as an opt out of sharing/sale, opt out of processing sensitive personal information, or both) and how far that signal extends (whether the business attempts to apply it to a specific user's account, to a specific browser, or only to the interaction in which the signal is received).

Furthermore, it would be extremely helpful for consumers to receive active feedback from a business when the business successfully processes an opt-out setting or signal. The CPRA requires implementing regulations *not* mandate a "notification or pop-up in responses to the consumer's opt-out preferences signal,"[17] which is important to prevent businesses from degrading the experience of consumers who do use such signals. However, the absence of *any* kind of visual signifier or feedback from the business could make it difficult for consumers to

[16] 11 CA ADC § 999.315(C)
[17] Cal Civil Code § 1798.185(a)(20)(B)(v)

"set and forget" a control like GPC and trust that it will serve as an effective communicator of their privacy preferences.

We request the Agency explore additional methods by which consumers could be informed as to the effectiveness of their choices exercised through global settings or opt-out signals. Rather than a pop-up notification, this could be in the form of a flag or label, unobtrusively located near the "Do Not Sell My Personal Information" link, or could be communicated back to the user's browser or device in some form. Another possibility is described in the draft GPC specification, which provides a way for websites that comply with GPC to communicate that fact by posting data at a "well known" URL. The data hosted at the URL allows browser extensions and similar tools to automatically audit a business's compliance with GPC.[18]

Additionally, we recommend that the annual reporting requirements for large businesses be expanded to include a delineation in reported opt-out requests made through browser signals which were interpreted as requests made by the consumer, opt-out requests made through browser signals which were interpreted as requests made by the device or browser, and opt-out requests made through alternative mechanisms.

Once again, the undersigned organizations appreciate the opportunity to comment on this initial rulemaking procedure. We welcome any comments, are available for additional feedback and look forward to continuing to work with the Agency as we move forward towards the ever-approaching date of CPRA implementation.

Sincerely,

Privacy Rights Clearinghouse
Access Humboldt
Becca Cramer-Mowder, ACLU California Action
Jacob Snow, Senior Staff Attorney, ACLU Foundation of Northern California
Common Sense Media
The Consumer Federation of America
The Electronic Frontier Foundation
Media Alliance
Oakland Privacy

[18] 4.1 GPC Support Representation, Global Privacy Control (GPC) Unofficial Draft 11 October 2021, https://globalprivacycontrol.github.io/gpc-spec/#gpc-support-representation (Last visited Nov. 8, 2021)