August 23, 2022

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd.
Sacramento, CA 95834

RE: Future of Privacy Forum CPPA Public Comment

Dear Mr. Soublet and Members of the California Privacy Protection Agency:

The Future of Privacy Forum ("FPF") welcomes the opportunity to comment on the proposed regulations to implement the California Privacy Rights Act of 2020 ("CPRA") amendments to the California Consumer Privacy Act of 2018 ("CCPA").[1] FPF is a non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies in the United States and globally.[2] FPF seeks to support balanced, informed public policy and equip policymakers with the resources and tools needed to craft effective regulation.

While FPF has a broad remit and expansive expertise across the field of consumer privacy, our comments here are focused on § 7025 of the draft regulations regarding opt-out preference signals ("signals") and are informed by an FPF review of mechanisms to convey 'Global Privacy Control' ("GPC") signals currently in the marketplace.[3] As the Agency's rulemaking process advances, we look forward to commenting on other important consumer privacy rights and business obligations established under the CPRA, including the definition and scope of "sensitive personal information."

The development and deployment of technological signals that communicate an individual's privacy choices to businesses can enable people to exercise their rights on an automated basis, significantly easing the burdens of privacy self management. The draft regulations resolve many ambiguities about the implementation, exercise, and impact of signals pursuant to the CCPA and reflect a nuanced understanding of both the opportunities and inherent limitations of such tools as they currently exist.

---

[1] California Privacy Protection Agency, "Text of Proposed Regulations" https://cppa.ca.gov/regulations/pdf/20220708_text_proposed_regs.pdf.
[2] FPF's comments do not necessarily reflect the views of FPF's supporters or Advisory Board.
[3] The Global Privacy Control has 7 "Founding Organizations" (two browsers: Brave, Firefox and five browser plug-ins: Abine, Disconnect, DuckDuckGo, OptMeowt, Privacy Badger) that transmit the signal, each with different user interfaces and different disclosures. https://globalprivacycontrol.org/. Additional, non-affiliated mechanisms can also transmit the signal, including the plug-ins Crumbs, Startpage Privacy Protection, and GPC Enabler.

As the California Privacy Protection Agency ("the Agency") proceeds in rulemaking under the statutory interpretation that the recognition of qualifying signals by covered entities is required by the CPRA amendments, addressing the following outstanding matters will help to ensure that Californians can reliably and easily exercise their CCPA rights through this emerging class of privacy controls.

A. Adopt rules for opt-out preference signals that provide clarity for websites while encouraging innovation in privacy controls for emerging digital and physical contexts.

In the fragmented consumer data ecosystem of web, mobile, smart TVs, Internet of Things, connected vehicles, immersive tech, and other emerging technologies, it is unlikely that a single, 'universal' signal specification will be developed that can effectively apply across all the digital (and physical) contexts in which individuals interact with businesses. For example, while specifications that transmit consumer privacy preferences through a web browser or browser plug-in, such as the GPC, are well-suited for conveying preferences to websites, additional signal specifications and mechanisms will be required to effectively invoke CCPA rights with other platforms and technologies, such as mobile applications and the range of consumer data platforms listed above.

FPF recommends that the Agency ensure that the final regulations and statement of reasons are sufficiently technology neutral to allow for and encourage the development of preference signals for non-website contexts. For example, draft regulation § 7025(a) provides that the purpose of preference signals is to enable the exercise of CCPA rights by "consumers interacting with businesses online." However, the CCPA's rulemaking grant does not specify that qualifying signals may only be developed or exercised in "online" contexts (*see* Civ. Code § 1798.185(a)(19),(20)). Final regulations should ensure that qualifying signals will not necessarily be applicable only to websites, but may be developed for mobile apps, connected products, and potentially govern data collected offline (such as from 'digital out of home' billboards).

Non-website privacy opt-out signals may seem far away, but in fact many are already in use or development. For example, the iOS and Android mobile operating systems have historically both provided the "Limit Ad Tracking" feature, involving a decentralized signal that communicates an individual's privacy preferences to mobile apps.[4] Similarly, researchers at Carnegie Mellon have developed a mobile privacy management tool designed to convey privacy signals to IoT devices.[5]

---

[4] *See* Bennett Cyphers, "How to Disable A ID Tracking on iOS and Android, and Why You Should Do It Now," Electronic Frontier Foundation (May 11, 2022), https://www.eff.org/deeplinks/2022/05/how-disable-ad-id-tracking-ios-and-android-and-why-you-should-do-it-now.

[5] Daniel Tkacik, "New infrastructure will enhance privacy in today's Internet of Things" CyLab (Feb. 19, 2020), https://cylab.cmu.edu/news/2020/02/19-privacy-assistant.html.

As user activity and data collection increasingly shifts to mobile and other non-website interactions,[6] innovations in privacy self-management tools will also continue.

Given the complexity and importance of establishing new specifications and processes governing data collection and sharing by traditional websites, it may be practical for the Agency's first set of regulations to address signal requirements as they apply to websites, browsers, and browser plug-ins (particularly through illustrative examples). However, in doing so, the Agency should ensure the promulgation of clear, non-technology specific principles that can encompass new privacy tools, including multimedia tools that can be recognized in emerging contexts and privacy dashboards that can provide pathways to multiple signal mechanisms.

B. Clarify and streamline requirements for businesses that "process" qualifying opt-out preference signals to avoid loopholes and ensure that disclosures are meaningful to average consumers.

FPF recommends three clarifications to the draft regulations concerning the requirements for how businesses are expected to respond to qualifying signals. First, the draft regulations should ensure that a business's leeway to ignore qualifying signals in order to respect a consumer's ongoing participation in a financial incentive program is appropriately tailored. The draft regulations establish a necessary 'consent hierarchy' for responding to signals that are in tension with other expressions of consumer choice. However, § 7025(c)(4) would create a potential loophole by permitting businesses to "ignore the opt-out preference signal" of a known consumer who does not affirm their intent to withdraw from a financial incentive program upon receiving notice of the conflict. The regulations should be clarified to specify that in such circumstances, a business may ignore a qualifying signal ***only with respect to that consumer's participation in the financial incentive program***, and not to any unrelated present or future sales or sharing of that consumer's personal information.

Second, the draft regulations should clarify the disclosures that businesses must provide regarding their receipt, processing, and implementation of opt-out requests. § 7025(c)(6) provides that a business "***should*** display whether or not it has processed" a consumer signal (emphasis added). The language appears permissive, especially when read in conjunction with other requirements in § 7025 that provide requirements for how a business "***shall***" respond to a valid signal. However, the Agency's Initial Statement of Reasons suggests that this provision is intended to be mandatory.[7] Final regulations should clarify whether or not businesses are required to display a signal status.

---

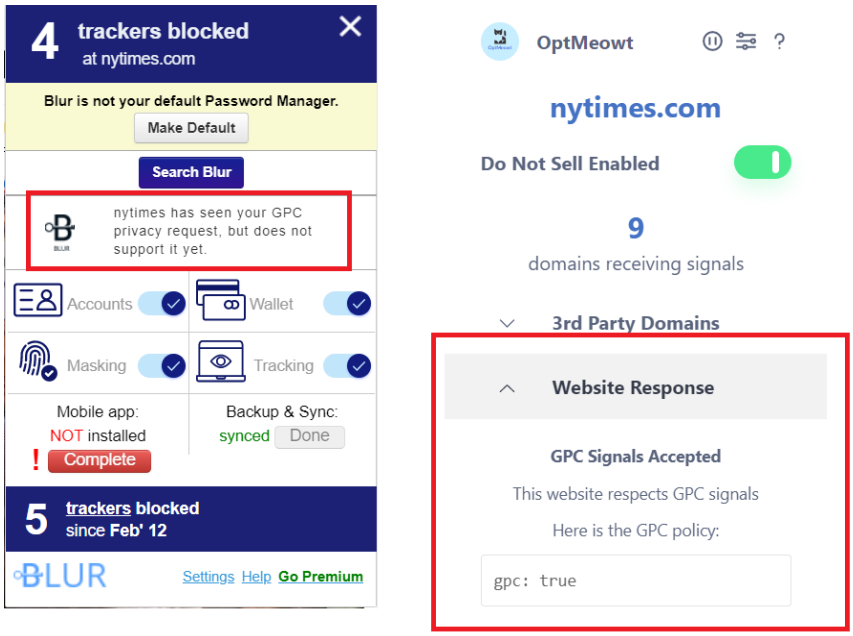
[6] For example, more Americans own a smartphone than a laptop or desktop computer. Pew Research Center, "Mobile Fact Sheet" (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/.

[7] California Privacy Protection Agency, "Initial Statement of Reasons" at 37: "Subsection (c)(6) requires a business to display whether a consumer's opt-out preference signal has been accepted, and provides exemplar language for how a business can communicate this information to the consumer" https://cppa.ca.gov/regulations/pdf/20220708_isr.pdf.

Third, final regulations should clarify how § 7025(c)(6) displays will interact with the related requirement under § 7026(f)(4) to allow consumers to confirm whether an opt-out request has been "processed," including through a display or toggle on the business's website.[8] For consumers, there will likely not be a meaningful distinction between displays indicating that: (1) a signal has been processed and (2) a request to opt-out has been processed. The regulations should avoid requiring businesses to unnecessarily 'conspicuously' clutter digital products and services by providing duplicative, potentially confusing displays regarding consumer opt-outs. Furthermore, the information on such disclosures could convey inconsistent information, as a business may "process" a signal set to opt-out of certain CCPA rights, but not implement it, if an expression of choice higher on the 'consent hierarchy' is present.

A simpler, more user-friendly approach would be for regulations to encourage businesses and signal providers to confirm a consumer's opt-out status directly through a signal mechanism, a feature that is already present in some GPC plug-ins, including OptMeowt and Blur (see Figure 1). These two plug-ins, in addition to displaying whether a signal was sent, also provide information on whether a recipient website respects or honors that signal. However, at present the disclosures can be inconsistent, possibly given that such browser tools remain in an early stage of development with respect to this particular signal and its legal status in California.

Figure 1: Blur and OptMeowt Plug-ins Display How a Website Responds to the GPC signal. *All screenshots taken August 19, 2022 on Chrome browser, Version 104.0.5112.81*



[8] § 7026(f)(4) "Providing a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business. For example, the business may display on its website "Consumer Opted Out of Sale/Sharing" or display through a toggle or radio button that the consumer has opted out of the sale of their personal information."

C. Encourage the further development of signal mechanisms that permit granular or business-specific consent choices.

In order to ensure informed consumer choice in the exercise of signals and as directed by the CPRA amendments' grant of rulemaking authority, final Agency regulations should provide guidance on mechanisms for enabling consumers to selectively consent for particular businesses to sell or share their personal information.[9] While the draft regulation's 'consent hierarchy' would establish processes for obtaining consumer consent that would override a qualifying signal in both non-frictionless (§ 7025(c)(3)) and frictionless (§ 7025(f)(3)) interactions, as envisioned these processes would occur separately from a signal or signal mechanism. Furthermore, § 7025(c)(5) of the draft regulations would prevent businesses from responding to a user's website-specific decision to disable a global opt-out signal. The regulations should encourage signal providers to develop controls that permit consumers to exercise their privacy preferences with respect to particular businesses.

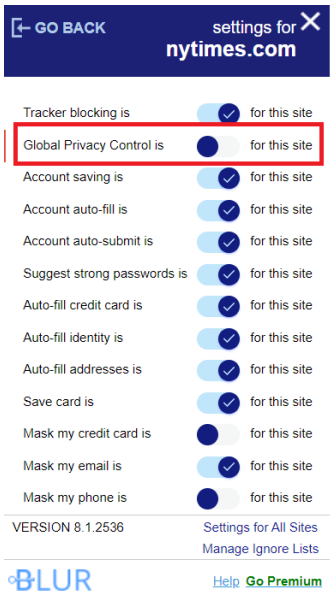
As drafted, the regulations would restrict the ability of signal providers, such as browsers and plug-ins, to offer granular, website-specific choice mechanisms to consumers, because § 7025(c)(5) holds that a business cannot interpret the absence of a previously received signal as consent to opt-in to the sale or sharing of personal information. In many cases this is a desirable policy outcome because simply visiting a website from a new browser or device without a signal mechanism installed or enabled should not override a previous expression of intent to opt-out. However, where an individual with a 'global' signal enabled engages with a business and then affirmatively chooses to disable that signal for that particular business, the regulations should permit the business to respect and implement that choice. The principle that affirmatively disabling an opt-out signal will have the impact reversing the signal's effect is intuitive, symmetrical, and easy to execute, consistent with the proposed requirements for consent contained in draft regulation § 7004. In fact, a requirement that if a consumer affirmatively disables a signal that action may not have the impact of disabling the signal would likely constitute an Agency-mandated "dark pattern," subverting user autonomy, decision making, and choice.

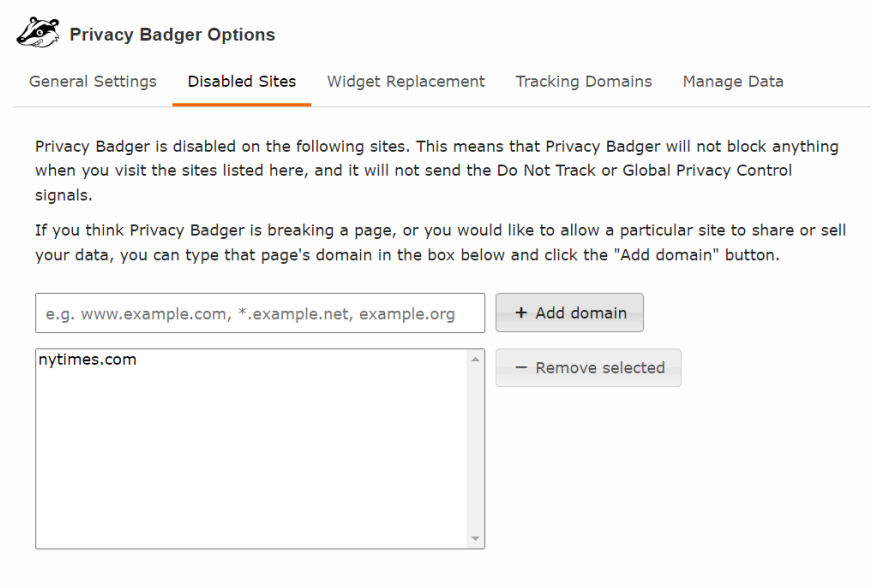
Notably, several plug-ins that have implemented the Global Privacy Control specification permit users to granularly enable or disable the signal for a particular business, website, or pages of a particular domain, including OptMeowt, Privacy Badger, and Blur (see Figure 2). Such controls can include functional buttons or toggles (for default-off signals) or a 'allowlist' of websites or domains

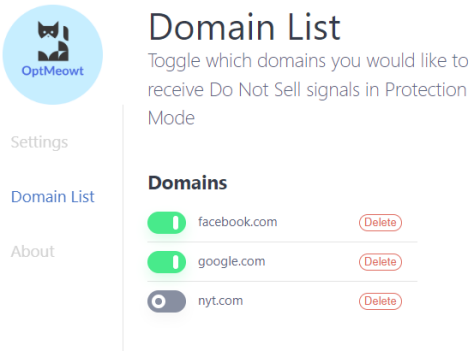
[9] Civ. Code § 1798.185(a)(19)(A)(v): "The requirements and specifications for the opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses, and should… Provide a mechanism for the consumer to selectively consent to a business' sale of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information, without affecting the consumer's preferences with respect to other businesses or disabling the opt-out preference signal globally."

(for default-global signal settings). Final regulations should support rather than override the existing ability for signal mechanisms to empower consumers to exercise their rights selectively.

Figure 2: Examples of Browser Plug-ins that Allow Domain-Specific Granular Controls (Blur, PrivacyBadger, and OptMeowt). *All screenshots taken August 19, 2022 on Chrome browser, Version 104.0.5112.81.=*







D. Revise the Initial Statement of Reasons to reflect CCPA requirements for ensuring consumer intent in the exercise of signals.

The CPRA amendments state that implementing regulations for signal requirements and specifications should "clearly represent a consumer's intent and be ***free of defaults constraining or presupposing such intent***" (Civ. Code § 1798.185(a)(19)(A)(v)) (emphasis added). However, the Agency's Initial Statement of Reasons contains a unique suggestion, not reflected in the draft

regulations, that businesses may be required to recognize "a privacy-by-default opt-out mechanism that is built into a platform, technology, or mechanism."[10]

In practice, whether or not a "privacy-by-default" setting in a browser or browser plug-in can be objectively determined to reflect a consumer's intent consistent with the requirements of the CCPA will be a context-specific inquiry. In making this determination and establishing guidance, the Agency should consider the browser or plug-in's primary advertised purpose, disclosures made to the user before and after installation, and whether the signal is configurable. Downloading a plug-in that has a primary advertised primary purpose that is unrelated to information privacy (such as a password manager, screen reader, or user-interface add-on) would be unlikely to satisfy CCPA's criteria if it were to incidentally send opt-out signals by default. However, a browser plug-in that is explicitly marketed as a tool to exercise consumers' legal rights to opt-out of the sale or sharing of personal information could satisfy the CCPA's requirement that signals clearly represents a consumer's intent. For example, the plug-in OptMeowt is currently described in the Chrome Store download page as allowing "Web users to make use of their rights to opt out from the sale and sharing of personal data" and has no functionality unrelated to sending the GPC specification.[11]

Browsers, unlike plug-ins, may require a more holistic analysis, given their necessary intermediary role between users and websites, the fact that most users have fewer options to choose from, and the multitude of reasons for which average users choose and continue to rely on their preferred browsers. Based on our analysis of the CCPA, it is unlikely that a browser, operating system, or multi-purpose device, even one that markets itself as generally protective of individual privacy, could enable an opt-out signal on behalf of its users in a way that would meet the Act's statutory requirements that signal mechanisms shall be free of defaults constraining or presupposing consumer intent. In general, the decision to adopt or use a particular browser is often based on a wide variety of factors including generally protecting privacy, but also features such as ad blocking, speed, user interface design, security, and safety.[12] It would be impraticable to infer, from objective factors, that an individual has chosen to use a browser or similar multi-purpose intermediary product due to a default 'do not sell or share' signal feature. Furthermore, the default enabling of signals by intermediary platforms would threaten to "unfairly disadvantage" other businesses, potentially selectively, in violation of Civ. Code § 1798.185(a)(19)(A)(i).

This is an important issue for the Agency to address because at least one existing web browser currently transmits the GPC by default without notice to users either on its download page or in

[10] ISOR at 34.
[11] Chrome Web Store, OptMeowt download page: https://chrome.google.com/webstore/detail/optmeowt/hdbnkdbhglahihjdbodmfefogcjbpgbo?hl=en-US.
[12] *See e.g.*, Michael Muchmore, "Edge, Firefox, Opera, or Safari: Which Browser is Best?" PC Mag (Apr. 4, 2022), https://www.pcmag.com/picks/chrome-edge-firefox-opera-or-safari-which-browser-is-best.

the browsers' settings, contrary to the CCPA's statutory requirements.[13] As browsers increasingly compete on privacy, the Agency should not look to whether a browser has obtained market dominance or widespread adoption before assessing whether its integration of opt-out preference signals unfairly disadvantages other businesses. Rather, the Agency should establish principled, objective factors – including, for example, examining the advertised purposes of a browser or tool, disclosures to users before and after download, and whether a setting is configurable, in determining qualifying opt-out signals.

E. Final regulations should enable users to exercise granular control over their privacy rights through opt-out preference signals.

The amended CCPA establishes three distinct consumer rights that may be exercised through opt-out preference signals, the rights to: (1) opt-out of data sales, (2) opt-out of data sharing, and (3) limit the use and disclosure of sensitive personal information (Civ. Code § 1798.120-121). The invocation of each of these rights may have different effects and potentially impact the functionality of products and services enjoyed by consumers in different ways. Therefore, it can be anticipated that consumers may wish to exercise different combinations of these rights through signals on either a global or selective (business-by-business) basis. Regulations should support such granularity of choice in a manner that is consistent, clear, and not overwhelming for users.

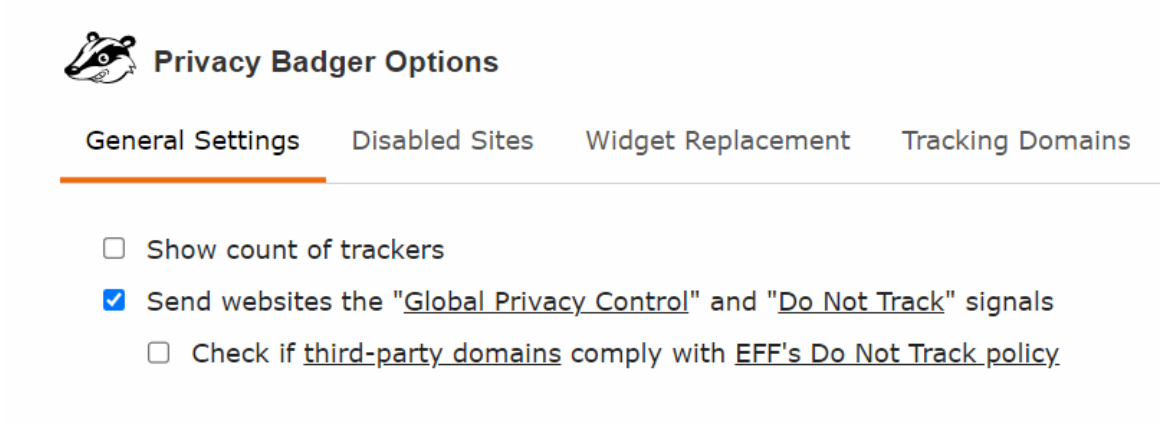
However, the current GPC specification, as developed for the CCPA prior to the CPRA amendments, only conveys whether the signal is enabled or not; it does not permit the granular exercise of underlying rights. Meanwhile, there are inconsistent disclosures in the current marketplace about what rights the GPC is intended to invoke. Some providers specify that the GPC will opt consumers out of data sales, while others portray that the signal will jointly invoke the right to opt out of both sales and sharing.[14] Furthermore, some plug-ins, such as the Privacy Badger, may constrain user autonomy by bundling the Global Privacy Control with other settings such as the 'Do Not Track' ("DNT") specification, without functionality that would permit users to disaggregate these features (see Figure 3).

---

[13] The Brave browser "does not require users to change anything to start using the GPC to assert your privacy rights. For versions of Brave that have GPC implemented, ***the feature is on by default and unconfigurable***" (emphasis added). Peter Snyder, "Global Privacy Control, a new Privacy Standard Proposal," Brave (Oct. 7, 2020), https://brave.com/web-standards-at-brave/4-global-privacy-control/.

[14] For example, Disconnect's help page (linked through the plug-in) states that: "The Enable GPC checkbox sends a Do Not Sell signal under the CCPA to sites you visit. The Global Privacy Control signal is experimental and non-binding." Alternatively, hovering over the GPC toggle on the Blur plug-in displays a statement that says "Requesting a site to not share or sell your data."

Figure 3: Privacy Badger Plug-in "General Settings." *All screenshots taken August 19, 2022 on Chrome browser, Version 104.0.5112.81.*



Recognizing that the Agency has postponed promulgating regulations on some statutorily-directed aspects of opt-out preference signals,[15] FPF encourages future Agency regulations to allow consumers to exercise granular control over their California privacy rights.

F. Establish an authoritative, multistakeholder process for the review and approval of qualifying signals and transmitting mechanisms

As signal specifications are developed and refined over time, new questions will arise as to whether a particular signal or signal-transmitting platform, technology, or mechanism meets the requirements of the CCPA and its implementing regulations. Consequently, FPF reiterates the suggestion in our November 2021 pre-rulemaking comments that the Agency establish an open, multistakeholder process for the ongoing review and approval of new signal mechanisms over time.[16] This process should include engagement with regulators in other jurisdictions that provide for the recognition of opt-out signals (particularly Colorado and Connecticut) in order to support as much interoperability as possible given underlying statutory differences in consumer rights, signal specifications, and consent hierarchies.

In addition to providing clarity for regulated businesses, active ongoing engagement from the Agency is uniquely important for California consumers and the developers of signal mechanisms. For consumers, public approval of either specific mechanisms (such as browsers and plug-ins) or the criteria for such mechanisms will allow them to have confidence that the specific tools they choose to enable will have real legal effect. It will also allow them to file complaints with the Agency for enforcement when they perceive that their requests are not being honored. For developers of platforms, intermediaries (browsers), and plug-ins, active Agency involvement will

[15] ISOR p. 33.
[16] Future of Privacy Forum "Comments PRO 01-21" at 9 (Nov. 8, 2021), https://fpf.org/wp-content/uploads/2021/11/Future-of-Privacy-Forum-Comments-PRO-01-21.pdf

allow them to continue competing on privacy while detecting and implementing qualifying signals in a way that meets California's legal requirements.

At the same time, it is important to recognize that a regulated entity that receives a signal may not be able to determine its specific source or transmitting mechanism (for example, whether the signal came from a user's browser, specific plug-in, a device setting, or other tool). In such cases, the signal source is relevant because the same specification or signal, such as the Global Privacy Control, could be implemented by providers or provided to consumers in ways that either do or do not meet the CCPA's requirements – and the receiving entity may have no way of distinguishing. In this situation, the Agency should actively discourage the non-compliant implementation of an otherwise qualifying signal while ensuring that businesses do not use the existence of non-compliant implementations of a small percentage of the total signals in the market as a justification to ignore all such signals.

***

Thank you for this opportunity to provide input on the Agency's initial draft implementing regulations for the California Privacy Rights Act amendments. We welcome any further opportunities to provide resources or information to assist in this important effort. If you have any questions regarding these comments and recommendations, please contact Keir Lamont at klamont@fpf.org.

Sincerely,

Keir Lamont
Senior Counsel

Jason Snyder
FPF Policy Intern