July 28, 2021

California Office of the Attorney General
Attorney General Rob Bonta
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Response to CCPA FAQ Regarding User-Enabled Controls and Related Enforcement Letters

Dear Attorney General Bonta:

The undersigned trade associations and organizations collectively represent a broad cross-section of the Californian and United States business community spanning various industries including advertising and marketing, analytics, magazine publishing, Internet and online services, financial services, package delivery, cable and telecommunications, transportation, retail, real estate, insurance, entertainment, auto, and others. Our organizations have a long history of supporting consumers' ability to exercise choice over uses of data for digital advertising. Enabling consumers to express their preferences and exercise control through easy-to-use, user-enabled choice mechanisms is a foundational aspect of data privacy that we have championed for decades. However, we are concerned that the OAG's new FAQ response regarding user-enabled global privacy controls will cause confusion for consumers and businesses, rather than effectuating genuine user choices.

In particular, we maintain the following three concerns. First, the FAQ mandate directly conflicts with the approach taken in the California Privacy Rights Act of 2020 ("CPRA"), which becomes operative in less than 18 months. Second, there was no public process for evaluating or

considering the cited tools or the particular implementations by the browser referenced in the FAQ, and as a result there are diverging perspectives around what constitutes a tool that is "user enabled." Finally, the existence of the FAQ unnecessarily prejudices a subject matter on which the California Privacy Protection Agency ("CPPA") is directed by law to promulgate rules. These concerns are compounded by the recent publicly-reported enforcement letters sent by the OAG to companies on adherence to such signals.[1] We therefore ask you to retract this FAQ response, reconsider your enforcement approach to user-enabled global privacy controls, and defer to California's new privacy agency on the subject.

- **The FAQ response conflicts with the approach taken in the CPRA. This will lead to confusion for consumers and businesses.** Not only does the California Consumer Privacy Act of 2018 ("CCPA") not direct the Attorney General to create and mandate adherence to the controls described in Section 999.315(c) of the regulations implementing the law,[2] but the FAQ response stands in direct contrast to the approach to such controls taken in the CPRA. According to the CPRA, businesses "may elect" to either (a) "[p]rovide a clear and conspicuous link on the business's internet homepage(s) titled 'Do Not Sell or Share My Personal Information'" **or** (b) allow consumers to "opt-out of the sale or sharing of their personal information… through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications to be set forth in regulations[.]"[3] Despite this choice that will become available to businesses in a short time, the FAQ response and decision to send enforcement letters to businesses regarding user-enabled privacy controls that do not align with the CPRA is unnecessary and creates confusion in the market. The OAG consequently takes a position on such controls that does not reflect California law and is likely to be different from the approach spelled out by new regulations implementing the CPRA. This will result in confusion for consumers and businesses.

- **The FAQ statement directly conflicts with the CPRA mandate explicitly directing California's new privacy agency to issue specific rules governing user-enabled global privacy controls.** The CPRA tasks the CPPA to issue particularized regulations governing user-enabled global privacy controls to help ensure consumers and businesses are protected from intermediary interference. Given the lack of formal process employed with respect to the OAG's proposed application of global privacy controls and the FAQ response, it does not appear that these safeguards have been considered and addressed. For example, the CPRA instructs the CPPA to "ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal *cannot unfairly disadvantage another business*."[4] According to the CPRA, the CPPA must also ensure user-enabled global privacy controls "*clearly*

[1] *See State of California Department of Justice, Rob Bonta Attorney General*, California Consumer Privacy Act (CCPA) FAQ Section B, #7 and #8, available at https://oag.ca.gov/privacy/ccpa; *see also* Kate Kaye, *California's attorney general backs call for Global Privacy Control adoption with fresh enforcement letters to companies*, DIGIDAY (Jul. 16, 2021), available at https://digiday.com/marketing/californias-attorney-general-backs-call-for-global-privacy-control-adoption-with-fresh-enforcement-letters-to-companies/.

[2] Cal. Code Regs. tit. 11, § 999.315(c); *see also* Joint Ad Trades Comments on the Second Set of Proposed Regulations Implementing the CCPA at CCPA_2ND15DAY_00310 - 00313, available here (noting California Administrative Procedural Act and constitutional concerns with Section 999.315(c) of the regulations implementing the CCPA) .

[3] CPRA, Cal. Civ. Code § 1798.135(b)(3).

[4] CPRA, Cal. Civ. Code § 1798.185(a)(19)(A) (emphasis added).

represent a consumer's intent and [are] free of defaults constraining or presupposing such intent."[5]

In contrast, the OAG's FAQ response does not ensure that any of the safeguards set forth in the CPRA's regulatory instructions are followed. For instance, the OAG's FAQ response lists a browser that sends opt-out signals by default without consulting the consumer, and such signals are unconfigurable.[6] The OAG's FAQ response therefore does not provide any means to enable businesses to determine whether a global privacy control signal, as implemented by particular browsers, is truly user-enabled, or if it is instead sent or communicated by an intermediary in the ecosystem without the consumer's consent. Moreover, the FAQ response contravenes the will of Californians, as expressed in passing the CPRA ballot initiative, that privacy regulation on the subject of user-enabled global privacy controls should come from the CPPA as opposed to the OAG.

- **New OAG guidance regarding user-enabled global privacy controls should be developed through a deliberative process that considers stakeholder input.** The OAG's FAQ response was posted to its website without any sort of formal deliberation or process prior to publication. Legal and material guidance such as those contained in the FAQ should only be issued after a carefully deliberated formal process that allows for public input. New rules or guidance regarding user-enabled global privacy controls should be afforded the benefit of a formal process, including public comment and thoughtful evaluation.

  Such process should also indicate how the OAG and/or CPPA will (i) ensure such controls are compliant with the CPRA, (ii) monitor control providers to ensure their compliance with law and the standards set forth in the CPRA, and (iii) set forth a system to ensure that modifications by browsers and other intermediaries remain compliant with law to avoid circumstances where changes "unfairly disadvantage another business" or no longer "clearly represent a consumer's intent and [are] free of defaults constraining or presupposing such intent." Issuing a rule on such controls without providing a deliberative process risks creating significant confusion and unworkable policy for consumers and businesses alike.

* * *

The undersigned trade associations and organizations fully support empowering consumer choice and advancing workable privacy protections for Californians. However, the position reflected in the OAG's recent FAQ response and enforcement letters was issued without formal process and contradicts the approach to user-enabled global privacy controls taken in the CPRA. We therefore respectfully ask you to reconsider the FAQ response, as well as your enforcement

[5] *Id.*

[6] *See* Brave, *Global Privacy Control, a new Privacy Standard Proposal, now Available in Brave's Desktop and Android Testing Versions*, available at https://brave.com/global-privacy-control/ ("Importantly, Brave 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.")

approach concerning user-enabled global privacy controls, and to instead defer to the CPPA on the issue. Please contact Mike Signorelli of Venable LLP at masignorelli@venable.com with questions on this letter.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
202-269-2359

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's
202-355-4564

Christopher Oswald
SVP, Government Relations
Association of National Advertisers
202-269-2359

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau
202-800-0771

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
703-220-5943

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
202-898-0089

Howard Fienberg
Senior VP, Advocacy
Insights Association
202-800-2545

Shoeb Mohammed
Policy Advocate
California Chamber of Commerce
916-879-7904

Lou Mastria, CIPP, CISSP
Executive Director
Digital Advertising Alliance
347-770-0322

Cameron Demetre
Executive Director, CA & the Southwest
TechNet
916-903-8070

Anton van Seventer
State Privacy & Security Coalition
202-799-4642

CC: California Privacy Protection Agency