401 Edgewater Place
Suite 600
Wakefield, MA 01880

December 28, 2020

Lisa B. Kim
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
Email: PrivacyRegulations@doj.ca.gov

Re: *OAL File No. 2019-1001-05: NOTICE OF FOURTH SET OF PROPOSED MODIFICATIONS TO TEXT OF REGULATIONS AND ADDITION OF DOCUMENTS AND INFORMATION TO RULEMAKING FILE*

Dear Ms. Kim:

Thank you for the opportunity to submit comments in response to the fourth set of proposed modifications made to the regulations regarding the California Consumer Privacy Act (CCPA).

The Me2B Alliance is a non-profit organization founded in 2019 with a mission of performing independent product testing/certification on connected technology—essentially measuring the ethical behavior of technology. Our primary ethos is that *respectful technology* is better for both people ("Me-s") and businesses ("B-s"). Our ethical foundation for *respectful technology* lies in what we call the Me2B Rules of Engagement, which mirror the attributes of healthy human inter-personal relationships.

Why use the characteristics of healthy human relationships as an ethical north star? Because we *are* in relationships with connected technology: it observes us, talks to us, interacts with us—just like people. When technology treats us with respect, it engenders greater trust in connected products and services, and the companies that provide them.

A crucial principle in the Me2B Rules of Engagement is *Respectful Defaults:*

> ***Respectful Defaults*** *- In the absence of stated preferences, we default to the most conservative behavior.*

Note this also aligns with the Privacy by Design principle: "Privacy as the default setting."[i] In particular, we strongly suggest that opting-in to information sharing or selling should

401 Edgewater Place
Suite 600
Wakefield, MA 01880

be the default standard for Web interactions; it reflects a more respectful default than requiring people to opt-out.

General Problems with Opting-Out

The current opt-out mechanism is problematic on multiple fronts:

1. It only applies to the "sale" of user data and not to sharing of user data, even though portable data can be shared with a service provider, who could sell the data without any notice or consent.
2. It places the burden on the individual to, in essence, opt-in to privacy, which fails to align with the human right of privacy; it also fails the principle of privacy as the default setting in Privacy by Design.
3. It presents significant difficulty in developing a global privacy signal standard, as the European Union in recent decisions has made clear that opt-out is not GDPR compliant.
4. Opting-Out presents a particularly confusing user interface (UI) in communicating a negative/opt-out (see also comments below regarding section 999.315).

In addition to the general comments above, the Alliance would like to submit its views on two discrete but important proposed changes to the draft regulations.

1. 999.306(b)(3): "sells" versus "collects"

Revisions to section 999.306, subd. (b)(3) would "clarify that a business selling personal information collected from consumers in the course of interacting with them offline shall inform consumers of their right to opt-out of the sale of their personal information by an offline method."

Part of this revision would alter the language in (b)(3) to cover a business that "sells" personal information, rather than "collects" such data from consumer.

This language change is troubling on several fronts. First, it greatly narrows the scope of covered interactions with consumers. Clearly "selling" is a subpart of data "collecting". Or to be more precise, "selling" is a specific use of data after the act of "collecting." We believe all people should be notified of information collection whether it's intended to be "sold" (CCPA definition) or used strictly in the context of the vendor/first party. This is particularly important during the national COVID pandemic, with known mobile data sharing from SDKs installed in apps, which are being shared through service provider loopholes and then sold by subsequent parties in the data supply chains without notice to users.

401 Edgewater Place
Suite 600
Wakefield, MA 01880

Second, "selling" is a more ambiguous term than "collecting." A company theoretically could evade the assumed intent of the provision by adopting a cramped definition of selling data.

Third, allowing data collection, even in the absence of sales, increases security risks for the user. Collection of data entails storing it on third party servers, where it would be subject to outside breaches and other harms.

Finally, while CCPA mostly restricts the "sale" of user data, and the newly-passed CPRA expands to restrict the "sharing" of user data, these two conflicting standards, without any technical consent-sharing mechanisms, present an impossible scenario for end-users or auditors to track the flow of their user data, and ensure that portable data isn't sold by parties who legally acquired the 'shared' user data under CCPA frameworks.

2. 999.315(f): the "opt-out button"

Proposed section 999.315, subd. (f) describes a uniform button (or logo) to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

Usability Issues with Opt-Out

Based on the findings of Cranor et al (listed as a resource in this round of proposed changes) which recommends an interactive simple text statement ("do not sell my data") without an icon as the most understandable UI per their testing, we are surprised to see the recommendation of an (untested?) generic checkmark icon.
From Cranor et al[ii]:

> *"None of the tested icons should be used to symbolize Do Not Sell. Instead, the link text should be used on its own or different icons should be developed and tested.... adding any of these icons to the link text introduced misconceptions regarding the opt-out button's purpose compared to presenting the link text on its own."*

It should be noted that the four icons tested by Cranor et al were all significantly more meaningful than the proposed check-mark button proposed in this revision.

In fact, using a checkmark with a negative statement sets up a particularly challenging UI for people, which is well understood in the art of UI design[iii].

Additionally, in another listed resource, "An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites""[iv]:

401 Edgewater Place
Suite 600
Wakefield, MA 01880

> *"In asking for consent, websites should present a clear, affirmative action, and ask visitors for agreement rather than incorporating the consent into default settings, such as pre-checked boxes (Art. 4)."*

We contend that mandating opting-out of selling data is tantamount to a default setting allowing the selling of data. Instead, people should be presented with a clear, affirmative [opt-in] action to ***allow*** the selling of their data.

Location of Opt-Out Signal on Infinite Scroll Pages

Furthermore, the suggested practice under CCPA to place a "Do Not Sell My Information" link in the footer of websites, is not possible for websites with "infinite scrolling" functionality, where new stories or content constantly populates as soon as a user scrolls to the bottom of the page where the footer links exist[v]. This concept also doesn't work on publishers with paywalls – where a user visits a page and is immediately both tracked and identified by javascript pixels on the page, but also unable to click on any elements besides the subscription notices to execute an effort to opt-out of any data sales. GDPR on the other hand, approaches consent from a position where a website can't use UI/UX tricks, locked-in pop-ups, infinite scrolling and other "scroll & click tricks" to collect consent or make it possible to opt-out. By making this "opt-out" instead of "opt-in," many users must sometimes navigate purposefully-broken websites that restrict clicks, scrolling, engagements (newspaper paywalls) and prevent users from being able to express their lack of consent for data sales.

Users Are Less Likely to Change Default Settings

Requiring people to opt out of selling their data is essentially a default setting that allows vendors to sell the data of users. Research shows that default settings favor whoever benefits from the default setting.

> *"The same applies to privacy settings, researchers have found in several studies.*
>
> *"Several possible reasons for not changing the default settings exist: cognitive and physical laziness; perceiving default as correct, perceiving endorsement from the provider; using the default as a justification for choice, lacking transparency of implication, or lacking skill," researchers from the Goethe University Frankfurt and Nelson Mandela Metropolitan University wrote in 2013."*[vi]

401 Edgewater Place
Suite 600
Wakefield, MA 01880

> *"If we assume that marketers, consumers, and policy-makers all share the goal of separating interested from uninterested consumers, our findings suggest some constructive advice regarding the role of defaults. In our research, defaults have a sizable effect, and the best way of controlling these effects may well be to neutralize them as much as possible."*[vii]

Changing to a Positive Statement

If we were to modify the confusing negative language of the proposed "Do Not Sell" button and instead reword it in a positive manner it would essentially be, "I want data privacy". This option should be tested and considered.

Opting-In Better Aligns with Judicial Opinions in the EU

Due to the maturity of the GDPR (relative to the CCPA), consent mechanisms have been more deeply scrutinized and tested in the European Union. Consent for data usage must be provided by "clear affirmative action"--i.e. opt-in. Whereas in the CCPA, the individual is defaulted into allowing the sale/sharing of information until they opt-out. The EU and Germany have upheld support for opting-in in the past year, affirming that opt-out is ***not*** valid consent.

From the Court of Justice of the European Union, October 2019[viii] [bold text below for emphasis and focus, not from original source]:

> *"In today's judgment, the Court decides that the **consent** which a website user must give to the storage of and access to cookies on his or her equipment **is not validly constituted by way of a prechecked checkbox which that user must deselect to refuse his or her consent.**"*

From the related case, May 28, 2020, the German Federal Court of Justice (*Bundesgerichtshof*, "BGH") decided on the "Planet49" case regarding cookies[ix]:

> *"The BGH ruled that Section 15 para. 3, sentence 1 TMA must be interpreted in light of and in conformity with Art. 5 para. 3 of the ePrivacy Directive as meaning that the use of cookies for creating user profiles for the purposes of advertising or market research **requires the user's consent**. Following the decision of the CJEU, the BGH **further ruled that the user's consent cannot be obtained by way of a pre-ticked checkbox which the user can uncheck**."*

And from the UK's ICO (Information Commissioner's Office), "Consultation: GDPR consent guidance", March 31, 2017[x]:

401 Edgewater Place
Suite 600
Wakefield, MA 01880

> *"**Clear affirmative action** means **someone must take deliberate action to opt in**, even if this is not expressed as an opt-in box. For example, other affirmative opt-in methods might include signing a consent statement, oral confirmation, a binary choice presented with equal prominence, or switching technical settings away from the default.*
>
> *The key point is that all consent must be opt-in consent – there is no such thing as 'opt-out consent'. Failure to opt out is not consent. You may not rely on silence, inactivity, default settings, pre-ticked boxes or your general terms and conditions, or seek to take advantage of inertia, inattention or default bias in any other way."*

Opting-In Eases Global Privacy Signal Standardization Efforts

Changing from opt-in to privacy to opt-in to selling/sharing data will align this important regulation more closely to the EU approach, which will facilitate the development of a global privacy signal standard. Currently, there is effort in the W3C to develop a global standard for a Global Privacy Control signal that is facing difficulties with reconciling a signal and a default setting that works everywhere.

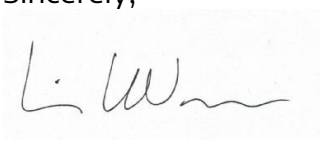
Recommendation

For the reasons stated above we strongly recommend changing the default from an opt-out of selling my data to opt-in to selling my data. Doing so will result in a privacy-respecting and Privacy by Design-compliant default, an easier to understand user-interface, and an easier path to a global privacy signal standard.

In the absence of this, positive language of the control/button (or logo) such as, "I want data privacy" (yes/no) should be evaluated.

On behalf of the Me2B Alliance, thanks again for the opportunity to provide feedback on this important regulation for California, the US and the world.

Sincerely,



Lisa LeVasseur
Executive Director, Me2B Alliance
Lisa.LeVasseur@me2ba.org

401 Edgewater Place
Suite 600
Wakefield, MA 01880

[i] https://en.wikipedia.org/wiki/Privacy_by_design

[ii] "CCPA Opt-out Testing – Phase Two", Cranor, Habib, et al, May 28, 2020. CCPA Opt-Out Icon Testing - Phase 2 - DNS (ca.gov)

[iii] Checkboxes - Checkbox label negating - User Experience Stack Exchange

[iv] "An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites", Habib, Zou et al, USENIX Symposium on Usable Privacy and Security (SOUPS) 2019. August 11–13, 2019, Santa Clara, CA, USA.

[v] https://oag.ca.gov/data-broker/registration/193828

[vi] **Default settings for privacy -- we need to talk" Albert Ng, December 21, 2019, CNET.** Default settings for privacy -- we need to talk - CNET

[vii] Defaults, Framing and Privacy: Why Opting In-Opting Out<Superscript>1</Superscript> (columbia.edu) Defaults, Framing and Privacy: Why Opting In-Opting Out

[viii] "Storing cookies requires internet users' active consent", Court of Justice of the European Union PRESS RELEASE No 125/19 Luxembourg, 1 October 2019 Judgment in Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände–Verbraucherzentrale Bundesverband eV v Planet49 GmbH.

[ix] "Germany: The decision of the German Federal Court of Justice on cookie consent – and further implications", *Global Compliance* News, Julia Kaufman, July 19, 2020. Germany: The decision of the German Federal Court of Justice on cookie consent - and further implications (globalcompliancenews.com)

[x] "Consultation: GDPR consent guidance", Information Commissioner's Office, March 31, 2017. draft-gdpr-consent-guidance-for-consultation-201703.pdf (ico.org.uk)