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

Dear Mr. Soublet,

I would like to comment on the regulations to implement the Consumer Privacy Rights Act of 2020. I am an assistant professor of computer science at Wesleyan University, where I direct the privacy-tech-lab [1]. Together with my students and collaborators I am working on privacy-enhancing technologies to enable people on the Internet to exercise their privacy rights effectively and efficiently. I am a co-creator of Global Privacy Control (GPC) [2], by which people can send requests to websites, apps, and other services to not sell or share their personal information with third parties. I would like to comment on §7025 Opt-Out Preference Signals.

1. **Clarify in the regulations that selecting privacy-preserving products or product versions demonstrates sufficient intent to opt out.**

   If people select privacy-preserving products, e.g., install Brave, Firefox, or DuckDuckGo Privacy Essentials, it can be unambiguously inferred that they want to opt out from the sharing and sale of personal information, cross-contextual advertising, behavioral profiling, and similar data monetization practices. The same is true for privacy-focused versions of a general product. Requiring the consumer in these instances to re-confirm their intent would be detrimental to the usability of opt-out preference signals and not serve any additional purpose. Thus, it would be preferable to clarify this point in the regulations as well.

2. **Further clarify in the regulations that the validity of a request to opt out of the sale or sharing of personal information does not require authentication or submission of additional information.**

   Whatever information a website, app, ad network, etc. uses to authenticate a user for purposes of data collection should also suffice for the authentication when exercising an opt out right. For example, if a website starts targeting a user simply upon visiting the site, all it should take for the user to opt out is to continue visiting the site with the opt-out preference signal enabled. The current practice of some sites to require additional information, e.g., name and email address, does not
facilitate the opt out if this information was not known by the site in the first place. Thus, for example, if a cookie ID is used to identify a particular user, all it should take for the site to facilitate the opt out is to associate that cookie ID with an opt out flag. It is not necessary to require authentication or additional information for that purpose. Any usability obstacles risk that the opt out right will not be effective. Thus, there is a risk that sections such as §7025(c)(2) (“However, a business may provide the consumer with an option to provide additional information ... .”) can be misused to degrade the usability of opt-out preference signals if sites misuse that option, for example, by extensively displaying opt out banners. It would be worthwhile to clarify that additional information can only be asked for for purposes of extending the opt out, for example, from one browser to all browsers a consumer is using.

3. Respecting opt-out preference signals must remain mandatory.

The single most important factor for broadly enabling people to exercise their opt out rights is to require recipients of opt-out preference signals to follow those. The experiences with the Do Not Track signal, for which the California Online Privacy Protection Act only requires disclosure of whether or not it will be followed, demonstrate how crucial the mandatory nature of privacy preference signals is. Thus, it is critical that the regulations remain clear on this point.

4. Implementing GPC is technically easy and various tools are available for website operators to enable people to opt out.

Some site operators express concern that GPC is challenging to implement. However, that is not the case. GPC is based on basic web technologies that are easy to implement. Various implementation guidelines are available online and many consent management platforms offer support for GPC. I worked with various site operators of sites big and small and helped them implement GPC. If there is a challenge, it is one of switching to a privacy-preserving business model.

5. Consider pointing to opt-out preference signal specifications that satisfy the requirements of the regulations.

It would be valuable for website operators to know which opt-out preference signals satisfy the requirements of the law. To that end, you could provide a website resource or otherwise provide such clarification.

Thank you for your efforts in moving privacy forward and the opportunity to comment. I am available for further questions and clarifications.

Sincerely,

Sebastian Zimmeck