Stanford Law School

Center for Internet and Society

Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610
Tel 650 723-5205
Fax 650 725-4086
cyberlaw.stanford.edu

February 25, 2020

To Whom It May Concern:

We are pleased to submit comments to the California Attorney General's office regarding the February 10th revision of the regulations for the California Consumer Privacy Act (CCPA). We make these comments on behalf of ourselves individually and provide our institutional affiliation for identification purposes only.

As researchers with expertise in information privacy and human-computer interaction, we share our concerns with aspects of the regulations as currently drafted, and offer suggestions we hope the AG's office will consider as you continue with this process.

Issue 1: The AG Should Not Adopt the Proposed Opt-Out Logo in the 2/10/20 Draft Regulations

In §999.306 (f)(1-3), the 2/10/20 version of the regulations include a proposal for the Opt-Out logo as required by the CCPA statute. Based on our expertise in human-computer interaction and design, we recommend the AG not adopt this design for the reasons we explicate below. Instead, the AG's office should either adopt the version recommended by the Carnegie Mellon (CMU) report[1], or alternatively, decline to adopt any logo for the final regulations at this time.

1. Background

Per the statute, §1798.185(4)(C) calls "[f]or the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information." We presume the authors of the original ballot initiative (later statute) reasoned that the opt-out of sale provision was significant enough that they desired to elevate and call attention to this option as compared to the other rights conferred by the statute. While this goal is laudable, it unfortunately opens a Pandora's Box of complex and competing issues with respect to visual signifiers and information privacy.

As the CMU report references, there have been multiple attempts over the years to signal privacy risks and options to consumers through the development and use of icons, including a set developed at Dr. King's institution, the Center for Internet and Society at Stanford Law School[2]. Unfortunately, none of these efforts have gained traction, in part due to a lack of incentives and regulation, but also because of the difficulty with

[1] Cranor, et al., *Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA* (February 4, 2020). Posted to the CCPA website.
[2] Cranor *et al,* Appendix A (p. 40).

representing the often complex concepts the icons attempt to capture. For example, explaining the practice of third party ad targeting through an icon to those who are unfamiliar with the concept is extremely difficult at best. As the CMU report details, there are many opportunities for misunderstanding on the part of consumers who know little to nothing about these practices. Add to the challenge an existing universe of competing icons and other signifiers (*e.g.*, browser lock icons, e-commerce verified merchant badges, etc.), and the Do Not Sell logo becomes yet another new element in an already crowded universe competing for consumer attention. Thus, one must raise the question of whether any logo for Do Not Sell will effectively inform consumers of this new right, especially if there remains no budget or plan for public education about the CCPA informing them of its existence.

2. The CMU Report Provides a Specific Recommendation Based on Credible Research

The CMU report provides a set of specific recommendations for the Do Not Sell logo based on a well-executed research study. The report calls for a "toggle" icon paired with a specific tagline ("Do Not Sell My Personal Information") to communicate the Do Not Sell right. Further, the report suggests a slightly different option to communicate the broader concept of privacy controls beyond Do Not Sell: the toggle icon paired with a "Privacy Options" tagline. We will not review this report in depth here, but we found the methods and analysis sound and the recommendations well-informed and appropriate. We do wish to highlight several findings from this report that are relevant to this discussion.

- *Privacy Options vs. Do Not Sell*: The report raises an issue which we think points to the need to consider a different option than what the statute requires: to not adopt any logo. While the report presents a clear path to follow to inform consumers about the Do Not Sell right, the report's discussion of a broader possibility, that of giving consumers a standardized method for locating privacy choices (beyond, but including, Do Not Sell), highlights an important need within the national (and even international) consumer privacy policy sphere to move beyond the "Privacy Policy" link (as mandated today by Cal-OPPA) and provide U.S. consumers with a discoverable and consistent means to inform them of where to find privacy-related information on any website or mobile app. The existing notice and consent framework, including privacy policies, privacy controls, and the methods in which we inform consumers of their existence, is in dire need of reform. This is a bigger problem than CCPA and Do Not Sell, and one that should be approached methodically, rather than piecemeal. To that end, we would suggest not adopting a Do Not Sell logo at this juncture in favor of pursuing the opportunity for comprehensive reform at either the state or federal level. That said, if the requirement to adopt a logo is read as absolute, then we suggest the toggle icon + Do Not Sell My Personal Information version as recommended by the CMU report.

- *Public Education:* As the CMU report argues, and as did Dr. King in her 2019 comments regarding the CCPA, we cannot expect consumers to broadly learn about and exercise these rights without a well-funded plan for public education. The development of a logo is no substitute for this problem. This lack of public education will particularly affect Californians living at the economic and social margins in our state. Absent a concerted public education effort, the Californians who do learn about the CCPA and their new rights will predominantly be those with access to media resources and education. Undoubtedly this will mean that the law will have a disparate impact, favoring those with higher incomes, education levels, technical literacy, and English proficiency.

- *Standardizing Do Not Sell/Deletion/Access Requests:* The CMU report, on page 34, suggests a standardized format for Do Not Sell requests that ensures they are simple, straightforward, and consistent. We endorse this approach and would suggest it also be considered for deletion and access

requests as appropriate. Since January 1st, Dr. King has been informally tracking CCPA notices and have observed a considerable diversity in terms of format, language, and even location on webpages. Some notices are even argumentative in their language, disputing the meaning of "sale" and suggesting the company is grudgingly complying with the law. Notices should not be a platform for arguing about the law. In order to provide consistency for consumers, the AG should require, or strongly suggest, the adoption of standardized notices for these new rights.

3. The AG Should **Not** Adopt the Logo In the 2/10/2020 Version of the Regulations

The logo included in the 2/10/2020 version of the regulations is problematic and should not be adopted. It is deficient in the following ways:

- *Confusing Design*: While the CMU toggle uses visual elements that are similar to an interactive button but do not replicate an existing design, the 2/10 logo appears to be based closely on the design of an Apple iOS toggle user interface element[3]. Thus, it raises the possibility for confusion among the public that the logo is an actual, interactive switch (rather than a logo or icon) that denotes a current system state. The CMU report raised the possibility of risk with their own toggle icon on page 31 of their report, though they found actual confusion to be very low[4]. The 2/10 logo inherently has this problem: in a very informal survey Dr. King conducted[5], when she showed individuals the 2/10 logo, all assumed it was an actual functioning button that indicated the current system state (set to Do Not Sell == yes). All assumed they did not have to take any action at all because the system default was set to Do Not Sell. In addition, according to general UI design guidelines[6], toggle switches should have an immediate effect and not require further "save" or "submit" action. Users may be confused if they try to click on the icon but do not see any change in the user interface. This may reduce the discoverability of the actual controls.

- *Color*: The 2/10 logo is red, which contributes to the confusion over its function. The individuals Dr. King asked about the logo assumed it was red because the button state was "on" (and that if Do Not Sell were inactivated, the button would be green or grey). Red is also a color generally reserved for critical errors in user interfaces; even using a red version of the proposed CMU logo would be problematic.

- *Dependency on a specific platform:* The toggle icon is a popular way to express the meaning of "control" due to its compatibility with mobile applications, wherein the primary interaction media is tactile. Therefore, the preferences of the toggle icon over other options may be a result of today's proliferation of mobile devices. However, the emergence of new consumer computing devices like virtual reality, augmented reality, and Internet of Things, may call for different interaction paradigms in the future, and affect the familiarity and interpretation of icons of the general public. The recommendation of an icon design tailored to a specific platform concerns us that future legislative updates may not be frequent enough to adapt to changes of perception. And even if the icons are updated in a timely manner, it can take a considerable amount of effort to make sure all websites and apps are also subsequently updated.

---

[3] https://developer.apple.com/design/human-interface-guidelines/ios/controls/switches/

[4] "[T]he *toggle* icon has a slight possibility of being viewed as an actual control (rather than a static icon) to give websites permission to sell data, which could deter users from interacting with it."

[5] Consisting of asking fewer than 10 people I personally know to look at the proposed logo and tell me what they thought its purpose was and how it functioned. This is not a scientific survey; however, within usability testing circles small-scale tests are a valid way of identifying critical user interface problems.

[6] https://www.nngroup.com/articles/toggle-switch-guidelines/

- *Source?*: Should the AG's office persist in recommending this logo, the source of the design, and any information related to its development and testing should be released in order to give researchers the opportunity to audit the development process. If the AG is in possession of evidence suggesting that this option is a better choice than what was suggested by CMU, then we should be able to review that evidence. In sum, no logo design should be adopted without user testing and research, and the results of those tests should be made public.

In sum, we strongly recommend that the AG adopt the toggle design with tagline that was recommended by CMU and do not adopt the version in the 2/10 regulations. However, we also suggest that there is a strong rationale for not adopting a logo at this juncture.

Issue 2: Mobile Notices

We are pleased to see the addition of §999.304(d)(4) to the CCPA draft regulations. Given the challenges of presenting notices on mobile devices, more clarity is welcome in this area. We would like to offer the following suggestions to further clarify this section.

1. Developer Engagement and Platform Involvement

The CCPA is targeted at companies that meet a threshold based on annual gross revenues or the centrality of information sales to the business based on either quantity or percentage of revenue. While these requirements likely exclude many small-scale mobile application developers, some will undoubtedly be subject to the law. The proposed mobile notice requirements appear to directly target large mobile developers as a major audience, as they propose specific language, icon, notice format (e.g. just-in-time notice) recommendations. These proposals have two requirements to make the law effective. First, developers should have sufficient knowledge and incentives to comply with the law. Next, an organization should be responsible to educate developers and audit their practices. A recent research study of privacy-related questions on software development question & answer sites showed that platform requirements are a more frequently mentioned driver (46% of sampled posts on the website Stack Overflow) than laws and regulations (only 2% of sampled posts)[7]. Platforms serve as an important force to drive developers to comply with legal requirements, and the CCPA can take advantage of their capabilities by making the role of platforms more explicit in the law. For example, platform app stores (e.g., mobile app stores, browser plugin stores, etc.) could take proactive steps towards detecting apps that lack a privacy policy on their app store pages and remind developers that these notices are required for California consumers of their apps, or even remove non-compliant apps from their app stores.

2. Specifying The Criteria For "Just-In-Time" Notices

The current regulation needs more specificity regarding the triggers for the just-in-time notice described in §999.304(d)(4). In part, this could be determined by more clearly explicating the purpose and limitations of the just-in-time notice: is it only for "personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect[8]," meaning any form of data collected from the consumer that is not demonstrably linked to the core purpose of the app? Would this notice apply only to the app developer, or to any

[7] Tahaei, Mohammad, et al. "Understanding Privacy-Related Questions on Stack Overflow." Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. 2020.

[8] While there is certainly extant research that maps the contours of what users expect from mobile experiences in order to define more precisely what consumers would not reasonably expect in a particular context, it is worth raising the question as to whether it makes sense to also define this requirement similarly to the GDPR's legitimate interest requirement. See: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504.

third-party library the app developer incorporates into the app that collects user information for ad targeting or other purposes outside the core functionality of the app? If it applied to both, who would ultimately be responsible for the notice? Further, would this notice appear every time a user opens an app, or just the first time?

The AG should be cautious in moving forward with this requirement to ensure that it does not inadvertently create a CCPA-version of the EU e-Privacy cookie notice, which has been the target of substantial criticism for subjecting EU internet users with routine cookie notices that are largely ineffective at offering users with any substantive choices, habituating the public to simply clicking "I Accept.[9]" However, the fact that it will not be present on every app may ensure enough novelty to avoid this issue, at least in part. That said, the inclusion of this new requirement raises the issue as to why only apps that are subject to the CCPA are targeted for this requirement, given that informing consumers of any app collection of personal information that is outside an app's core functionality is important for all app users to know.

In order to create a consistent user experience, platform providers (e.g., Apple for iOS, Google for Android) could implement the design and presentation (based on public input/feedback) of just-in-time privacy notices and their subsequent choices (e.g., selecting Do Not Sell) by providing a centralized interface, also known as a "native" user interface, that developers cannot change. Further, platform providers could provide developers with methods to specify the moments their app collects information from its users in a machine-readable format. Information provided in this way should be treated equally to information in privacy policies, for which developers should be held accountable for its accuracy.

In sum, this new provision could be an effective tool in raising consumer awareness about information collection in excess of what apps require for functionality. However, the existing language needs more specificity regarding the purpose of the notice and aspects of its functionality.

Issue 3: General Issues with CCPA Notices

The 2/10 version of the regulations raise several issues around notices that we think may require some additional clarification. We present them here in no specific order.

1. Providing New Notices

Section 999.304(d)(6) states that: "A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection." In response, we ask whether businesses will be required to inform consumers who have already viewed or consented to a previous notice. Will consumers be required to re-consent or acknowledge the new terms of collection?

2. CCPA and Cal-OPPA

Sections 999.305(a)(2)(a-d) lay out several rules regarding how companies must provide CCPA notices, while §999.308(a) provides guidelines for privacy policies. We ask whether these requirements will govern all privacy policies for California consumers, or only those companies subject to the CCPA? This regulation appears to

[9] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (*CCS '19*). Association for Computing Machinery, New York, NY, USA, 973–990. DOI:https://doi.org/10.1145/3319535.3354212

require that businesses with existing privacy policies that are now subject to the CCPA will also have to update their privacy policies to meet these requirements. Given that Cal-OPPA provides no requirements to businesses about the clarity of the language in a privacy policy, this appears to be a new requirement that may benefit consumers. Furthermore, §999.308(b) appears to conflict with Cal-OPPA regarding the proscription of the precise wording of the "privacy policy" link itself ("The privacy policy shall be posted online through a conspicuous link using the word 'privacy,' on the business's website homepage or on the download or landing page of a mobile application.") Will the CCPA requirements preempt those of Cal-OPPA? If yes, this opens the possibility to companies exploring other options for privacy policy links beyond "privacy policy," such as the "Privacy Options" language recommended by the CMU report. If this is the case, we would caution the AG to be specific in explicating exactly what terms can be used to avoid companies entitling the links with terms such as "Privacy Benefits" or "Privacy Choices" when the "benefits" and "options" available to them are fictional or lack substantive choice.

3. Notices to Minors

Sections 999.331 and 999.332 include directives regarding notices to minors. As currently written, these sections do not include any language that requires companies to produce notices for minors that are written at a comprehension level using language that children can understand. Without such a requirement, we are likely to see notices written for well-educated adults that are beyond the grasp of children to understand. To that end, we recommend the AG's office review the Age Appropriate Design Code recently drafted by the U.K. Information Commissioner's Office. In particular, we recommend standard #4:

- **"**Transparency**:** The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated."[10]

Our concern is that without such a requirement, notices to minors will be ineffective. Requiring companies to both write notices at a level of understanding for minors, as well as potentially including links to content educating minors about data privacy and related issues, both creates an ineffective regulation as well as a missed opportunity to educate children about data privacy and data protection.

Thank you for the opportunity to submit these comments.

Sincerely,

Dr. Jennifer King (via email)
Director of Consumer Privacy
Center for Internet and Society, Stanford Law School

Tianshi Li (via email)
Ph.D. Student
Human-Computer Interaction Institute, Carnegie Mellon University

[10] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/