California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

Re: Comments on Assembly Bill 375, the California Consumer Privacy Act of 2018

March 29, 2019

To Whom It May Concern:

We are pleased to submit comments to the California Attorney General's office regarding AB 375, the California Consumer Privacy Act (CCPA). We submit these comments on behalf of ourselves individually and provide our institutional affiliation for identification purposes only.

The CCPA, as passed, includes provisions that we are concerned will ultimately be ineffective in protecting consumer privacy. We describe our concerns in detail below.

1. <u>This law includes design-based directives that are not supported by existing research.</u>

California is not unique in its efforts to pass laws that include digital design imperatives that are not vetted by design experts, and thus in their implementation may be ineffective, or at worst, contravene the intent of the law. In the absence of a requirement for evidenced based policy-making, California legislators may pass legislation that includes design-based directives that are created *ad hoc* without supporting expert research. In the domain of computer interface design, these ad hoc choices may have unintended effects. For example, research conducted by Dr. Jennifer King and colleagues[1] has demonstrated that CalOPPA's 2003 requirement that all websites conducting business with California residents include a link on the website's homepage with the specific wording "Privacy Policy" has contributed to consumer confusion over the meaning of the phrase itself, with consumers reporting a mistaken belief that the phrase "Privacy Policy" implies an actual level of privacy protection that in fact does not exist.

In Section 1798.135(a)(1), the CCPA specifies that businesses "provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information." How will businesses interpret this 'clear and conspicuous' link requirement? Existing implementations of CalOPPA suggest an answer. CalOPPA gives specific requirements regarding the appearance, content, and placement for links to a company's privacy

[1] See: Hoofnagle, Chris Jay; King, Jennife;, Li, Su; and Turow, Joseph. How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? (April 14, 2010). Available at SSRN: https://ssrn.com/abstract=1589864; Turow, Joseph; King, Jennifer; Hoofnagle, Chris Jay; Bleakley, Amy; and Hennessy, Michae., Americans Reject Tailored Advertising and Three Activities that Enable It (September 29, 2009). Available at SSRN: https://ssrn.com/abstract=1478214

policy. The net result has been that the vast majority of websites place the link in the footer (at the bottom) of their homepages and across their Web sites—arguably not a conspicuous placement, and one that signals the link's relative unimportance in relation to other elements on a Web page. Doubtless we will see the 'Do Not Sell' link relegated to the same placement, where it will join "Privacy Policy," "Your California Privacy Rights," and other mandated links. Given that the current definition of "homepage" in 1798.140(l) includes "any Internet Web page where personal information is collected," businesses will likely need to place a link on every page of a website (and potentially mobile app) due to the fact that both websites and mobile apps often include pervasive advertising trackers that collect personal information from consumers across most or all of a website's or app's pages, irrespective of whether the website or app itself is actively collecting user information.

It is important to note that placing these links at the bottom of a Web page is neither inherently clear nor conspicuous, and is *not based on any research suggesting what the optimal placement would be for consumers to both notice and comprehend these links.* Furthermore, CCPA assumes that the best presentation for this form of notice is a link, as opposed to any other form of interaction, constraining the form of notice and potentially making it future-incompatible, particularly as voice-based interfaces become more common. CCPA, like CalOPPA, contains inherent assumptions about how to communicate notice to consumers about privacy without any reference to the decade-plus research efforts in this area to determine how best to do so. As such, it may contain the seeds of its own ineffectiveness by reifying a paradigm of notice that research has demonstrated repeatedly that consumers ignore or misinterpret.

2. <u>Educating consumers about their new deletion rights will require considerable effort, which appears both unaddressed and unfunded in CCPA.</u>

In order for this law to be effective, the public must know that it exists and how to act on it, specifically what rights they have, and how to exercise them. California must provide public outreach and educational materials informing consumers of the CCPA. However, the existing legislation is silent on the matter of consumer education, and appears to not contain any mechanisms for funding such education. We must not assume that consumers will naturally understand what these new rights are or how to use them. Furthermore, should our predictions in Section 1 be accurate and the 'Do Not Sell' link is relegated to website footers, *most consumers will not know this right exists*. Public knowledge of the 'Do Not Sell' or 'Deletion' rights will become dependent upon media coverage and outreach by civil society organizations, filling in the gaps left by a lack of public outreach by the State of California.

The inclusion of Section 1798.185(a)(3)(C) ("*For 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."*) attempts to address the issue of public knowledge by calling for the development (by whom?) of a consistent logo or button to increase consumer awareness of the 'Do Not Sell' right. But absent an accompanying public relations or education campaign, the mere existence of this button or logo does not guarantee that the public will be well-informed of this new right. Further, this button or logo will compete against an already crowded field

of privacy and security seals, as well as other visual elements competing for one's attention. Assuming a button or logo is an effective means of informing the public of this new right, what would be the most effective way of displaying it in relation to the link requirement? If most companies do display the 'Do Not Sell' link at the footer of their page, should this button/logo be placed near it? Or somewhere else? How should it display on mobile Web pages? Or within mobile apps? Or, what would be the most effective way of communicating this information to consumers, period? Unfortunately, while experts such as ourselves can make research-based suggestions to attempt to optimize this requirement, ideally we would have the ability to review these proposals before the law's passage, or even better, be provided with the time and resources to design and test possible solutions to make formal recommendations to the State.

3. <u>CCPA, as written, focuses on first party relationships, but is silent on how consumers will identify the companies that acquire and sell/share their data.</u>

While consumers may understand who the first party businesses are who collect their data, what is particularly unclear to the majority of the public is who else is collecting information about them. This is a category of actors that include advertising technology (Adtech) businesses, data brokers, and others who collect, buy, sell, and trade in consumer data, typically without consumers' tacit knowledge or express consent. Consumers generally do not have direct relationships with these businesses. As written, CCPA makes assumptions around notice that presupposes consumers will know exactly which companies they wish to target to exercise their 'Do Not Sell' and 'Deletion' rights. How will consumers determine which companies hold their identifiable or household data outside of the first party business relationships they have initiated directly?

One solution could be for first party businesses to publicly identify the companies (and include contact information) to whom they sell or share data (and thus potentially obviate Section 1798.83., a.k.a. The Shine the Light law[2]), as well as the companies for whom they facilitate direct data collection from consumers (*e.g.*, Adtech companies). The original text of the ballot initiative included a similar provision, and it is regrettable that the current legislation does not. Another solution could be found in the European Union's General Data Protection Regulation (GDPR): businesses have to actively inform a consumer within a reasonable time period that they are processing their data and from which source the data originates.[3]

This requirement should extend to any business that collects data facilitated by a first party relationship. Compliance with this requirement would ensure that the websites and mobile apps that utilize advertising technology services must identify all of the parties collecting their customers' data.

[2] See: Hoofnagle, Chris Jay and King, Jennifer. Consumer Information Sharing: Where the Sun Still Don't Shine (December 17, 2007). Available at SSRN: https://ssrn.com/abstract=1137990.
[3] See GDPR art. 14(1), (2)(f) and recital 61, http://data.europa.eu/eli/reg/2016/679/oj

4. CCPA, as written, does not appear to provide consumers with meaningful deletion rights with respect to Adtech-type businesses.

The deletion right provided by the CCPA makes the most sense when considering consumers' direct relationships with information-collecting businesses (*e.g.*, Facebook, Google, etc.). In these cases, a consumer can make an affirmative decision to end a relationship with a specific company or website and thus request the deletion of her data. Looking forward, the company or website presumably would not continue to collect data about the individual, unless the individual consumer re-initiated a relationship.

However, when considering businesses such as Adtech companies that collect consumer information through another company's website or app, this deletion right appears misleading. Given that consumers today typically do not affirmatively consent to, or are even aware of, these 'secondary' relationships, what will be the practical effect of initiating a deletion request with one of these businesses? Our concern is that these companies can restart the collection process as soon as a consumer visits a website or uses an app that deploys their services. Assuming an individual could even keep track of the myriad of secondary companies that silently collect her personal information, if an individual consumer wishes to prevent further collection of her information by these secondary businesses, she would have to know which websites and apps engage with the primary companies she engages with. Furthermore, for the deletion requests to be meaningful, she would potentially have to track herself to whom and how often she had made deletion requests and then judge how often she would need to repeat the requests. A scenario such as this calls into question the efficacy and meaningfulness of the deletion right itself.

It would seem most sensible to switch our engagement with information collection in California to opt-in, rather than opt-out, much like the GDPR has. However, we are aware of the potential legal challenges to an opt-in regime in the U.S., and the CCPA may not be the best avenue by which to make this challenge. At the same time, it is exactly this form of data collection and tracking that consumers dislike the most, and it does not appear that the CCPA, as currently conceived, will have a meaningful effect on this problem.

5. The 'Deletion' and 'Do Not Sell' rights that the CCPA creates run the risk of not being effectively enforced.

While consumers are given the right to civil action in security-related cases, they do not have such a right when businesses do not comply with their consumer right requests. The only sanction those businesses face is a civil penalty of a maximum of $7,500 per violation, asserted by the Attorney General. Given that there is no formal mechanism for consumers to lodge a complaint with the Attorney General, it is unlikely that even in the event a business categorically ignores consumer right requests and therefore commits multiple violations, such a civil penalty would significantly multiply. Under the current sanction regime of the CCPA it is—at least for bigger companies—cheaper to simply not comply with most provisions of the law and pay an occasional penalty than it would be to

comply with them. This not only renders the law itself ineffective and poses a risk to the rule of law, but also disadvantages smaller businesses. These upfront calculations of intermittently paying a small penalty rather than actually abiding the privacy law is what had been happening in the EU for decades, and which led to the sensible and dynamic fines under GDPR.

We would therefore recommend amending the CCPA to (1) re-introduce the right to civil action for consumers who have suffered any kind of violation of the CCPA; (2) increase the maximum civil penalty to an amount that will reasonably deter violations; (3) re-introduce the right to lodge a complaint with the Attorney General; (4) and, re-introduce enforcement by additional public entities.

6. Further harmonization of CCPA with the GDPR.

After having spent immense efforts into complying with the GDPR over the last years, many California businesses have a significant interest in capitalizing on the synergies between the CCPA and the GDPR. Though the CCPA does entail concepts inspired by the GDPR, it often comes short of the GDPR's full force of effect This becomes particularly apparent in regard to the right to deletion. In order to improve the CCPA, in addition to addressing the specific concerns we list above, we therefore also suggest the following, non-conclusive alignments:

A. Extend the right of deletion to personal information irrespective of its origin.

Other than the GDPR, the CCPA only allows for consumers to request the deletion of their personal information from businesses that themselves collected the information. Once a consumer's information is sold to or shared with a third party, the consumer has no means of having it deleted. With the objective of the CCPA being to give consumers more control over the use of their personal information, the current wording remains largely ineffective to achieve this goal.

B. Introduce joint liability.

While a business has to direct its service providers to delete personal information after receiving a deletion request, it is not liable for the non-compliance of its service provider with this direction. Therefore, there is no incentive for a service provider to actually follow this direction. Following the GDPR's example, we would suggest the incorporation of a joint liability of the business and its service providers for the deletion in order to ensure the effectiveness of the provision.

C. Narrow the exceptions for compliance with deletion requests.

Currently, there are three exceptions to the obligation to delete personal information that seem to bear the risk of being excessively invoked by businesses and therefore hinder the provision to grant consumers an effective right of deletion, namely Section 1798.105(d)(1), (7) and (9). Again drawing from the GDPR, we would suggest to instead introduce the concept of 'legitimate interest' as an exception for when a business may deny a deletion. This way, businesses would have to consider the implications of a continuous processing of personal information on the right to privacy of the

consumer. Only where the individuals' interests and fundamental rights and freedoms are outweighed by the businesses' legitimate interests, they would be exempted from fulfilling deletion-requests.

7. California can be a leader in shifting the paradigm of notice and consent.

While there is much debate about how best to legislate privacy, there is nearly universal agreement that how we inform the public about the use of their data is ineffectual at best and misleading at worst. We know that privacy policies are generally unread by the public; they are too long and written for lawyers, by lawyers; their language is often ambiguous and elides over specific uses of consumer data. In sum, they are unhelpful for providing consumers with clear, actionable data for making informed decisions. It is no wonder that researchers have documented a sense of resignation among the public regarding the use of their personal data.[4]

While California led the U.S. by passing CalOPPA in 2003 and requiring that websites post privacy policies for California consumers (and, by default, most of the globe), at the same time it gave companies a minimum standard with which to comply that has proven to be ineffective at providing the public with clear, actionable knowledge by which to make informed decisions. As written, CCPA does nothing to address or improve this state of affairs, and in fact enshrines existing flawed notice and consent principles into new law.

There are two approaches we suggest here: the first makes specific suggestions with regards to notice and consent to aid CCPA as written. The second makes big-picture recommendations as to how California can lead in shifting the paradigm around privacy disclosures.

A. CCPA-Specific Suggestions

1. Pursuant to Section 1798.185(a)(6) ("*Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter.*"), we recommend that the Attorney General and the Legislature consider engaging directly with academic researchers, civil society organizations, and Human-Computer Interaction/User Experience Design practitioners to solicit recommendations as to how best to design and implement the notices required by this statute following principles of user-centered design. This engagement could take the form of a formal working group or advisory committee, or a design challenge, for example. The critical requirement is to initiate a formal process that these communities can respond to with a goal of influencing policy; absent this incentive, these communities are not likely to engage in the policymaking process, given that

[4] See: Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. New Media & Society. https://doi.org/10.1177/1461444819833331

academic publishing generally does not reward policy-focused research, and practitioners are unlikely to engage in *pro bono* work without a specific client. Relatedly, the State could also directly commission a research study to achieve these ends.

2. Require that all businesses post standardized language (titles and text) that describe the 'Do Not Sell' right, the process for making a request, and any additional information for consumers. Absent these requirements, companies may be incentivized to use language that misleads consumers. However, we suggest that this language is developed based on a user-centered design process as suggested in (1) above.
3. Amend the definition of "homepage" in Section 1798.140(l) to include the following: "The application's platform page or download page (within an online store and/or on a website), a link within the application" to ensure that apps that are available both through online stores such as Google Play as well as directly on company or personal websites are included.
4. Amend Section 1798.135(a)(1) to include all of a company's digital interfaces (e.g. all mobile applications and mobile websites, in addition to standard websites), and to include information about the right in printed materials accompanying any Internet connected hardware or devices that lack interfaces (e.g., connected devices, such as appliances, or 'smart speakers') or where presenting a link is impracticable.

B. Fundamental changes to the Notice and Consent Framework

While researchers have been examining the problems with notice and consent for nearly two decades, there has been neither federal or state-level efforts to distill these findings and create either recommendations or actual legislation that translates this research into a new framework that aims to make notice standardized, clear and consumer friendly, and gives consumers substantive and meaningful consent options. While the Federal Trade Commission has held workshops[5] exploring the issues around notice design and consent, and has issued guidance for design issues related to disclosures generally,[6] they have not issued guidance beyond their 2012 *Protecting Consumer Privacy in an Era of Rapid Change* report, where they suggested "[p]rivacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices."[7]

California could take a lead in this challenge, by following the suggestions in 7(A)(1) above to commission expert guidance and feedback that addresses both the CCPA specifically and to spark action towards rethinking how we can improve notice and consent mechanisms that effectively inform consumers and give them real and significant choices over their personal information. In order to create a truly privacy-forward law that provides the public with meaningful, actionable rights, the CCPA's notice requirements should not rest on an existing framework that fails to properly inform consumers and provide them with substantive consent processes. Should we eventually see

[5] https://www.ftc.gov/news-events/events-calendar/2012/05/short-advertising-privacy-disclosures-digital-world

[6] See the FTC's Dot Com disclosures guide: https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf

[7] https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

action on these issues at the federal level, California's work in this area would serve as a model as to how to reconstitute how we provide notice and obtain consent in the digital world.

In closing, we appreciate this opportunity to submit our comments and provide the Attorney General's office with feedback on this important law.

Sincerely,

Dr. Jennifer King*
Director of Consumer Privacy
Center for Internet and Society
Stanford Law School
jenking@law.stanford.edu

Jana Gooth, MLE*
Visiting Research Scholar
Center for Internet and Society
Stanford Law School
gooth@stanford.edu

*Affiliation provided for identification purposes only. These comments are not submitted on behalf of the Center for Internet and Society.