Aug 22, 2022

Before the
California Privacy Protection Agency,
State of California

CPRA Public Comment

Thank you for the opportunity to provide comments on the proposed regulations of the California Privacy Rights Act. We are academic researchers associated with the University of Chicago and Northwestern University who focus on privacy. We draw on our collective experience in computer science and law to encourage the California Privacy Protection Agency to resist watering down the strong and sensible protections established by the proposed regulation. We also offer some concrete suggestions to enhance transparency, efficiency, and clarity in the regulations. We recognize the importance of the proposed regulation not only for the protection of Californian's privacy but also as a model for other jurisdictions.

1. **General Support of the Proposed Draft**

First, we commend the Agency for expanding the regulatory provisions that protect consumer privacy. There are a number of changes that we feel the Agency included that will significantly improve consumer privacy. We highlight a subset of these changes here. Defining and including Sensitive Personal Information (SPI) as a new category of personal information to be protected similar to the European Union's Special Category Data under Article 9 of GDPR. The Agency opted to expand on the EU's category to include additional sensitive consumer data like text messages and emails, further protecting consumers from unwanted surveillance. The Agency expanded the rights to know/access/opt-out given to consumers by the CCPA to now also include not just the selling of consumer data but also the sharing of consumer data. We strongly support this change, as the unsolicited sharing of personal information can be as much of a violation of privacy as selling it. The CPRA also includes new rights not included in the CCPA such as the right to rectify incorrect information and the rights to access information about the use of personal data in automated decision making ('profiling') and to opt-out of

automated decision making. Lastly, the Agency added necessary provisions that specify obligations for third parties/contractors/service providers, filling potential gaps in the consumer data life cycle.

2. Standardized Access and Site Location

As Internet researchers, we are familiar with the large differences in approaches to policy that platforms use. The language adopted, navigability, and accessibility to establish these policies are all a matter of variance by platform. We recognize the provisions that enforce Ease of Understanding, Symmetry, Straightforward Language, Ease of Execution, and Providing Instructions, but we suggest the Agency considers including a clause approximating Easy to Find. Easy To Find is crucial for usability since prior research has shown, for instance, that even when privacy options are available to users, if they cannot find them, they are often unused. Even further, the Agency could enforce a standardized location for information and disclosures. For example, all information relevant to these regulations could be accessible from www.[platform].com/privacy. Standardizations such as this one would make it easier for consumers to exercise their rights, agencies to perform auditing, researchers to study platform practices and policies, and allow companies to not have to make all new decisions from a blank slate. Further, without such standardizations, companies may continue to bury their options in a variety of settings forcing consumers to intuit their way through sometimes unintuitive settings (some unintuitive interfaces may still not be considered full-on dark patterns). The Agency may also consider going even further to smoothen the transition for company compliance, such as providing compliance guidelines like the guidelines provided by the FTC or EU.

3. Section 7002's Connection to Consumer Expectations Improves Transparency and Predictability in the Law

The proportionality principle embedded in Section 7002 is a beneficial approach for privacy regulation. Proportionality is a concept that is central to various domains of domestic data privacy law. See, e.g., Christopher Slobogin, Privacy at Risk: The New Government Surveillance and the Fourth Amendment (2007); Margot E. Kaminski, Privacy and the Right to Record, 97 Boston Univ. L. Rev. 167 (2017); Lior Jacob Strahilevitz, Reunifying Privacy Law; 98 Cal. L. Rev. 2007 (2010). Proportionality has become central to the GDPR approach to regulating personal data in Europe as well. See Miriam Kohn, Clearview AI, TikTok, and the Collection of Facial Images in International Law, 23 Chi. J. Int'l L. 195 (2022). It is also at the core of the duty of loyalty contained in the proposed federal privacy law.

The proposed regulation provides very helpful clarification about how firms and regulators will conduct proportionality analysis by incorporating consumer expectations. What kinds of collection, use, retention, and sharing data is expected by an average consumer is an empirical question. Fortunately, it is one that scholars have studied in great depth and with increasing sophistication. See, e.g., Kirsten Martin & Helen Nissenbaum, Privacy Interests in

Public Records: An Empirical Examination, 31 Harv. J. L. & Tech. 111 (2017); Roseanna Sommers & Vanessa K. Bohns, The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance, 128 Yale L.J. 162 (2019); Lior Jacob Strahilevitz & Matthew B. Kugler, Is Privacy Policy Language Irrelevant to Consumers?, 45 J. Legal Stud. S69 (2016). Empirical researchers have coalesced around best practices, including the need for the replication of research results and the formulation of expectation questions to respondents in a neutral way.

A great virtue of the empirical approach is that it enables regulated firms to anticipate the content of government regulation and enforcement. That is, if firms are uncertain about the application of proportionality review to an emerging technology they are considering employing, they can, at a moderate cost, employ the tools that disinterested academic researchers have been using to assess the expectations of their customers, or consumers generally. Some privacy-invasive practices are consistent with consumer expectations and others are sharply inconsistent with them, and firms' business practices and user-interfaces can alter those expectations. See Sara Katsanis et al., A Survey of U.S. Public Perspectives on Facial Recognition Technology and Facial Imaging Data Practices in Health and Research Contexts, 16 (10) PLOS One (Oct. 14, 2021); Matthew B. Kugler, From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms, 10 U.C. Irvine L. Rev. 107 (2019). Making the expectations of an average consumer an important part of the regulatory inquiry permits firms to engage in profitable practices that leverage the economic value of consumers' data. But it requires these firms to be highly transparent about what they are doing so that consumers who object to those practices can make an informed decision to take their business elsewhere.

This is not to say that a firm that conducts surveys and experiments to assess the relationship between a particular business practice and consumer expectations is in the clear and can claim a safe harbor under the regulation. Firms that employ hired guns with social science training to produce biased, self-serving survey and experiment results should not be permitted to engage in unnecessary and disproportionate privacy-invasive practices. Rather, if a firm conducts a serious and fair-minded investigation of consumer expectations before launching a product or engaging in a new practice and determines that its contemplated actions are consistent with most consumers' expectations, it is quite likely that the same results will be obtained months or years later when a regulatory entity evaluates consumer expectations. That is because citizens' privacy expectations tend to be stable over time. See Matthew B. Kugler & Lior Jacob Strahilevitz, The Myth of Fourth Amendment Circularity, 84 Univ. Chi. L. Rev. 1747 (2017). The proposed regulations' expectations-based approach thus makes the content of the law transparent and relatively easy to anticipate. Under Section 7004(a)(4)(C) of the proposed regulation, this tie to consumer expectations also enhances transparency and predictability in the definition of dark patterns.

Well-run firms already invest in learning what their customers want and expect. The proposed regulation provides further legal compliance incentives for firms to understand their current and potential customer base. Coupled with the CPRA's disclosure obligations, this increases the efficiency of the market in sorting consumers across companies.

4. Section 7004's Symmetry in Choice Approach is Appealing

There is little question that dark patterns are proliferating online. See Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Paloma & Alberto Bacchelli, UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception, Proceedings of the CHI Conference on Human Factors in Computing Systems (2020); Arunesh Mathur, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty & Arvind Narayan, Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Sites, Proceedings of the ACM Human-Computer Interaction Conference (2019). There is also a growing empirical literature examining the effects of dark patterns on consumer choice. See, e.g., Colin M. Gray et al., End User Accounts of Dark Patterns as Felt Manipulation, ACM Computer-Human Interactions Conference Proceedings (2021); Jamie Luguri & Lior Jacob Strahilevitz, Shining a Light on Dark Patterns, 13 J. Legal Anal. 43 (2021); Stefan A. Mager & Johann Kranz, On the Effectiveness of Overt and Covert Interventions in Influencing Cookie Consent: Field Experimental Evidence, 42nd International Conference on Information Systems (2021); Midas Nouwens et al., Dark Patterns after the GDPR: Scraping Consent Pop-up Ads and Demonstrating their Influence, CHI Conference Proceedings (2020). These studies reveal that particular dark pattern techniques successfully manipulate consumers into purchasing goods or services that they do not wish to purchase, retaining subscriptions that they prefer to cancel, or surrendering personal information that they prefer to keep private. See Luguri & Strahilevitz, supra and Nouwens et al., supra. Dark patterns further engender feelings of frustration as consumers feel manipulated. See Gray et al, supra.

The dark pattern examples identified in the regulation are among the most pernicious techniques currently employed in e-commerce. For example, the use of double-negatives is highly effective in manipulating consumers, with consumers often signing up for services they believe they have rejected. Nagging, obstruction, visual interference, confirmshaming, default terms, and fine print have been demonstrated to be quite effective at convincing consumers to sign up for dubious services without sparking a substantial consumer backlash, as long as the techniques are used subtly and in moderation. See Luguri & Strahilevitz, supra. The proposed regulations' examples provide helpful context for market participants who are trying in good faith to comply with the law.

While dark patterns are a broad phenomenon, the asymmetry present in user interfaces often indicates the presence of a dark pattern. Thus, a company may permit customers to sign up for a subscription in one click but require customers to mail a letter via snail mail or navigate

through multiple screens to cancel. That structure will rarely be accidental, and even if the asymmetry results from an innocent design mistake, its ongoing effects should be obvious. Hence Section 7004's emphasis on symmetry of choice is wise.

To be sure, there will be instances in which it is appropriate for a firm to introduce some modicum of friction. For example it would make sense for an email provider to ask "Are you sure?" before deleting a customer's account and all of their emails, provided confirmshaming and other one-sided techniques are not employed. Such a screen reduces the probability that an unwanted outcome will result from an errant click. But a firm can avoid any concerns about liability for introducing such friction by introducing a symmetrical "are you sure?" prompt at the account creation stage. Beyond that clarification, we offer several suggestions to improve the proposed regulation's symmetry in choice framework.

First, we recommend expressing Section 7004(a)(2) in terms of consumer effort as well as the number of steps necessary to opt in or out of sharing. A choice architecture that allows users to opt out of the sale of their personal information through two clicks on pages that require a typical consumer to read 1000 words of text and allows users to opt in to the sale of their personal information through two clicks on pages that require a typical consumer to read 100 words of next is not symmetrical. Consumer effort includes both the number of screens a consumer has to click through and the time it will take a typical consumer to read the materials pertinent to making a well-informed choice. Symmetry in choice should permit regulators to evaluate friction introduced in interface design from the perspective of both the number of steps necessary to make a choice effective and the time required for a typical consumer to do so.

Second, we recommend clarifying that symmetry of choice principles are applicable to Section 7026(j)'s discussion of CCPA opt-outs. It is asymmetrical for firms to ask consumers who have opted out of personal information sharing to opt-in every twelve months if those firms do not also ask consumers who have opted in to personal information sharing whether they wish to opt out every twelve months. It would be symmetrical for firms to either respect any initial consumer choice until the customer affirmatively requests a different choice or to provide every consumer with an annual decision about whether to continue or change their current choice.

Third, special care should be taken when constraining firms' choice of default terms. Section 7004(a)(2)(E) provides that a "choice where the option to participate in a financial incentive program is selected by default . . . is neither equal nor symmetrical." Default terms are inevitable in some instances so as to ensure that consumers are not overwhelmed with an excessive number of choices. A firm that implements a default term that is demonstrably desired by the majority of its customers or potential customers has not employed a dark pattern. For example, many credit card issuers provide their customers with 1% cash back on all card purchases. A credit card issuer that enables cash back by default (or that makes cash back a

mandatory condition of participating in the card program) rather than forcing customers to affirmatively opt-in to receiving cash back should not be construed as having violated Section 7004(a)(2)(E). Empirically sound customer surveys along the lines of those described in our discussion of Section 7002 can help firms establish that particular default provisions are desired by most of their customers and therefore permissible.

5. Kid Friendly: 7070-7072

Sections 7070-7072 pertain to the special provisions for consumers under the age of 16. We stress the importance of protecting privacy related to vulnerable populations such as children. The provisions say little about how the options or disclosures should be presented to children. We recognize that Section 7004 requires consent language to be easy to understand, but we submit that language for children may require additional consideration. If information is required to be given to children, it needs to be in a way that is understandable to them, as children may not understand the same language that is directed for adults.

* * *

As platforms mine consumer data to increase user engagement and financial gain, the CCPA and CPRA can serve as important sources of protection for Internet users. The Agency can aid users by raising awareness about privacy and the dark patterns used to undermine it, providing more rights to consumers, and keeping companies accountable through enforcement and audits. As research suggests, correcting the asymmetry in privacy choices and enforcing better privacy defaults are likely to significantly increase consumer privacy. Meaningful regulation is necessary to protect consumer autonomy and welfare. We are available to assist the Agency towards the goal of protecting user privacy amidst the dominant economic systems commodifying consumer data.

Respectfully submitted,

Marshini Chetty
Assistant Professor, Department of Computer Science, University of Chicago

Matthew Kugler
Associate Professor of Law, Northwestern University

Brennan Schaffner
Graduate Student, Department of Computer Science, University of Chicago

Lior Strahilevitz
Sidley Austin Professor of Law, University of Chicago Law School

Contact:

https://cs.uchicago.edu/people/marshini-chetty/
https://www.law.northwestern.edu/faculty/profiles/MatthewKugler/
https://cs.uchicago.edu/people/brennan-schaffner/
https://www.law.uchicago.edu/faculty/strahilevitz