Privacy Rights Clearinghouse


Consumer Federation of America

COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION, ACLU CALIFORNIA ACTION, PRIVACY RIGHTS CLEARINGHOUSE, OAKLAND PRIVACY, CONSUMER FEDERATION OF AMERICA, AND MEDIA ALLIANCE

to the

CALIFORNIA PRIVACY PROTECTION AGENCY
On Proposed Rulemaking Under the California Privacy Rights Act of 2020
(Comments on Modified Text of Proposed Regulations)

November 21, 2022

Introduction

Our groups are writing in reply to the invitation issued by the California Privacy Protection Agency ("the Agency") seeking input from stakeholders in developing regulations as directed by the California Privacy Rights Act (CPRA), and the California Privacy Protection Act (CCPA) as modified by the CPRA. These comments are in response to the version of rules that the agency published Nov. 8, 2022.

About The Parties

The **Electronic Frontier Foundation** (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. With over 35,000 dues-paying members (with several thousand California members) and well over 1 million followers on social networks, we focus on promoting policies that benefit both creators and users of technology. EFF has engaged in discussions around privacy regulations in California and throughout the country at the state and federal level. EFF has previously submitted comments to the California Attorney General regarding rulemaking for the California Consumer Privacy Act (CCPA), both as an individual organization and in collaboration with other leading privacy advocacy organizations.

ACLU California Action protects civil liberties and civil rights, advances equity, justice, and freedom, and dismantles systems rooted in oppression and discrimination. ACLU California Action has an abiding interest in the promotion of the guarantees of individual rights embodied in the federal and state constitutions, including the right to privacy guaranteed by the California Constitution and the right to due process. ACLU California Action is a 501(c)(4) organization associated with the three ACLU affiliates in California—

ACLU of Northern California, ACLU of Southern California, and ACLU of San Diego and Imperial Counties.

Privacy Rights Clearinghouse is focused on increasing access to information, policy discussions and meaningful rights so that the right to data privacy can be a reality for everyone. Founded in 1992 to help people understand their rights and choices, it is one of the first and only organizations to focus exclusively on data privacy rights and issues. For three decades, our team has been driven by the beliefs that data privacy is a fundamental human right and essential for an equitable future, and that everyone deserves the opportunity to be informed and be heard.

Oakland Privacy is a citizen's coalition that works regionally to defend the right to privacy, enhance public transparency, and increase oversight of law enforcement, particularly regarding the use of surveillance techniques and equipment. As experts on municipal privacy reform, they have written use policies and impact reports for a variety of surveillance technologies, conducted research and investigations, and developed frameworks for the implementation of equipment with respect for civil rights, privacy protections and community control.

Media Alliance is a Bay Area democratic communications advocate. Our members include professional and citizen journalists and community-based media and communications professionals who work with the media. Our members are concerned with communications rights, especially at the intersections of class, race and marginalized communities.

The Consumer Federation of America (CFA) is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education. Today, more than 250 of these groups participate in the federation and govern it through their representatives on the organization’s Board of Directors. CFA is a research, advocacy, education, and service organization. As an advocacy

organization, CFA works to advance pro-consumer policies on a variety of issues before Congress, the White House, federal and state regulatory agencies, state legislatures, and the courts. We communicate and work with public officials to promote beneficial policies, oppose harmful ones, and ensure a balance debate on issues important to consumers.

Reiterating Concerns about "Financial Incentives" in §7016

In our previous comments we made several recommendations to ensure that consumers had strong rights. In cases where the Agency has made changes to sections we have previously discussed, we build upon those recommendations below.

There is one concern we outlined in previous comments that has not been addressed in the latest version of the draft rules. Section 7016 addresses financial incentives that businesses offer to consumers to hand over their personal information to the business. This practice is commonly referred to as "pay-for-privacy," as the net effect on the consumer is often paying a higher price for a good or service if they choose to make the privacy-protective choice.

We remain disappointed that draft regulations leave mostly untouched the extreme license given to businesses to compute "the value of the customer's data" according to almost any formula or method that they might choose. The lack of specific guidance will likely result in a crazy-quilt of methods to measure the value of the customer's data to the business. The statute requires the incentive to be "reasonably related" to the figure the company provides, but these regulations fail to provide a standard to ensure that the value number itself is reasonable. Thus, these regulations leave room for companies to come up with figures that may be completely unreasonable values for customers' data so long as the financial incentive the company provides is reasonably related to the unreasonable value the company gives the

data. For a financial incentive to be reasonably related to an unreasonable value computation seems neither reasonable nor protective to consumers.

We reiterate our recommendation that the Agency consider providing some sample computations of the value of a consumer's data to a business, as you have provided examples in a number of other sections of the draft regulations. The examples can and should include an example of a reasonable method to arrive at a value number as well as an example of an unreasonable method.

Such examples should also include acceptable additional business purposes for acquired customer data that clearly meet the "reasonable consumer expectation" standard and examples of those that would not meet the "reasonable consumer expectation" standard.

Comments on New Changes To Regulations Published On Nov. 8, 2022

As privacy advocates, we are concerned about several changes to the regulations that appear to set up additional barriers to consumers' ability to exercise their rights under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).

Changes to Definition of "Disproportionate effort"

Changes to the definition of "disproportionate effort" will make it easier for businesses to refuse to fulfill valid consumer requests to know and correct information, and to refuse to pass those requests on to third parties with which they have shared information. In our previous comments, we asked that this definition be changed to prevent people being put in a situation where a business defines what "benefit" such a request may provide to them.

The updated definition shifts the balance of power even more in favor of businesses by allowing businesses to decline to comply with requests based on their evaluation of the

"reasonably foreseeable impact to the consumer by not responding." It also remains unclear to us what the consumer's appeal rights will be when a business informs a consumer that their request will not be fulfilled because the effort to the business is disproportionate to the benefit they will receive.

The Removal of Illustrative Examples in § 7002(b)

During the written comment period for the first draft of these Regulations we applauded the Agency for including illustrative examples throughout the draft that clearly indicated the Agency's intent and provided well defined guard-rails for businesses to follow. The removal of illustrative examples in § 7002(b) makes it easier for businesses to mislead and confuse consumers, reduces the clarity of the regulations, and weakens the protections of the CCPA.

Where there was a clear standard based on a reasonable consumer's reasonable expectations and a series of examples indicating what violations of that expectation could look like, now there are multiple multi-element tests that still leave as much in question as a reasonableness standard. Relying on, for example, "the strength of the link" between a consumer's reasonable expectations at the time of collection and "the other disclosed purposes" requires the same reasonableness analysis, but introduces an additional layer of uncertainty, compounded by the lack of clear illustrative examples of what could constitute a violation. In light of their inclusion and subsequent removal from the draft it also introduces confusion as to whether the Agency considers, for example, a mobile flashlight application that collects consumer geolocation information without the consumer's explicit consent to be in accordance with the section 7002 restrictions on collection and use.

Illustrative examples provide concrete representations of the regulations as applied, a crucial illustration of the Agency's intent, and in many cases were based on real-world

privacy-invasive business practices that these regulations are attempting to address.[1] We urge the agency to reinstate the illustrative examples that were removed in section 7002(b).

The removal of illustrative examples in § 7004(a)(2)

The removal of the illustrative examples in § 7004(a)(2)(D) & (E), has the effect of significantly weakening the principle of "symmetry of choice" and striking an essential category of dark patterns.

As defined in the OECD's report on *Dark Commercial Patterns*: "**Interface interference**: . . . [gives] visual precedence to options favourable to the business, thus creating a false hierarchy."[2] § 7004(a)(2)(D) & (E) are examples of interface interference giving visual precedence to more favorable business options, and further, explicitly illustrated how "the path for a consumer to exercise a more privacy-protective option shall not be longer or more difficult or time consuming than the path to exercise a less privacy-protective option". The removed illustrative examples could just as easily be considered "preselection variants" of the "Asymmetric Choice" dark pattern outlined by the FTC staff report, *Bringing Dark Patterns to Light*.[3]

Striking these examples is antithetical to the findings, intents and purposes of the CPRA ballot initiative as well, which acknowledged that information asymmetry makes it difficult for consumers to "at a glance" understand what they are exchanging and therefore difficult or impossible to negotiate with businesses; that businesses and consumers should be

[1] Federal Trade Commission, *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers*, (Dec. 5, 2013) available at https://www.ftc.gov/news-events/news/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived-consumers.
[2] OECD, *Dark Commercial Patterns*, OECD Digital Economy Papers, 10 (Oct. 2022), available at https://www.oecd-ilibrary.org/science-and-technology/dark-commercial-patterns_44f5e846-en.
[3] Federal Trade Commission, *Bringing Dark Patterns to Light*, 25 (Sept. 14, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

given clear guidance about their responsibilities and rights; and that the law should empower the consumer to be able to negotiate with the business on equal footing.[4]

Allowing businesses to preselect a "yes" choice or more prominently display the choice to participate in a financial incentive program will compound the problems identified above, make it easier for businesses to mislead consumers, undermine the intent of the ballot initiative, and would be a significant weakening of these Regulations from the first draft. For these reasons and others we urge the agency to reinstate the removed illustrative examples from § 7004(a)(2).

Changes to § 7004(a)(4) reduces clarity and significantly weakens the protections against dark patterns.

In § 7004(a)(4), removing "manipulative language" is antithetical to the spirit of the section and the CCPA. "Manipulation" has been a critical component of dark patterns since the term's inception. From the FTC's *Bringing Dark Patterns to Light*, "Coined in 2010 by user design specialist Harry Brignull, the term 'dark patterns' has been used to describe design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm."[5] By only prohibiting language that would "impair or interfere" consumers' choice, it removes a class of dark patterns that are designed to nudge, manipulate, or influence. For example, in the Norwegian Consumer Council's report *Deceived by Design*, they detail Facebook's attempt to roll out face recognition technology by highlighting all of the positive sides of data sharing when prompting users to give their

[4] The California Privacy Rights Act, SEC. 2(F), (H); see also SEC. 3(B)(1), (C)(2),(3).
[5] *Bringing Dark Patterns to Light*, *supra* note 3, 2.

consent. On the flip side, Facebook framed opting-out of data sharing as dangerous or risky.[6] As written, the regulations would not cover this type of dark pattern.

Instead, the Agency would have to rely on § 7004(c) to determine whether this practice is "substantially subverting or impairing user autonomy" as a backstop, undermining the clarity and proactivity that the regulations are meant to provide. Disconnecting this principle from the concept of manipulation will make it easier for businesses to use dark patterns and mislead consumers. We urge the Agency to recenter the concept of "manipulation" in § 7004(a)(4).

§ 7004(c). Requiring a business's intent to be a factor that must be considered in determining whether a user interface is a dark pattern is costly and reduces clarity of the regulations.

Adding business intent in § 7004(c) as a factor creates a larger administrative burden for the Agency, as the Agency would presumably need access to the organization's emails, meeting minutes, and other documents in its attempt to construct intent. It also incorrectly shifts the focus from a practice's impact on end-users to a business's culture and internal procedures.

Additionally, development of dark patterns is increasingly being done without any human interaction: "[B]usinesses are moving toward the use of artificial intelligence both to design and target digital materials. At some point, no human will need to be directly involved. The only discernible business intent is likely to be intent to maximize business

[6] Norwegian Consumer Council, *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy* (Jun. 27, 2018), 22, available at https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-designfinal.pdf.

metrics such as click rates, sales, or retentions. No human needs to intend to deceive or know that the design is deceptive."[7]

§ 7011. Privacy Policy

We had not previously provided comment on the changes to this section, which significantly weakened the ability for all people to access and understand business privacy policies. The Agency previously did considerable work to ensure that every consumer, regardless of their ability or language skill, would have a reasonable chance of being able to access and understand these policies. To only require that it be in a format that "allows a consumer to print it out as a document" is a major step back from the goals of accessibility laid out in the original rules.

Removing Requirements to Notify Consumers About Third Parties at Point of Collection and Requirements to Notify Third Parties About Consumer Requests.

The latest draft of regulations remove an obligation for businesses to notify people about which third parties the business allows to control personal information. These regulations also, at several points, weaken or remove requirements for businesses to notify third parties about consumer requests—particularly requests to opt out of sale and sharing, requests to limit the use of sensitive personal information, and requests to delete information. While the Agency has pointed to revisions of §7052 and §7053 as the reason for these changes, we respectfully disagree that those sections serve the same utility to consumers as those that have been altered or removed.

Removing the §7012(e)(6) obligation for businesses to notify consumers at the point of collection about which third parties may also control their data, or information about their

[7] Lauren E. Willis, *Deception by Design*, 34 Harv. J. Law & Tech. 115, 158 (2020).

business practices, makes it substantially more difficult for any consumer to understand what will happen with their information after it is collected. Transparency is the first step toward empowering consumers to exercise their privacy rights. The CCPA and the CPRA, in a majority of circumstances, already place the onus on consumers to seek out and file requests with every company that may hold their information. Removing this notice makes this process an even more burdensome guessing game for consumers.

Furthermore, responsible businesses that properly safeguard consumer data should know how information they collect flows to third parties. Stating this at the point of collection should not be difficult for businesses, and doing so makes exercising rights substantially easier for consumers.

Additionally, changes to §7022 (b, c) could narrow the instances in which businesses must notify service providers or contractors about consumer deletion requests. Rather than covering any information "obtained in the course of providing services," the draft rules now only cover information that is specified in a written contract between businesses and their service providers or contractors, or that businesses have "enabled" these third parties to collect.

In its explanation of the change, the Agency notes that this alters the "language to be more precise about how the service provider's or contractor's obligations apply to the personal information it collected pursuant to the written contract with the business." This narrowing, however, potentially allows for third parties to retain information they may collect in the course of doing business but that is not specifically enumerated in any written agreement, even in light of a deletion request.

Of perhaps greater concern are changes to §7026(f)(2) and §7027 that remove any requirement to notify third parties of requests to opt out of sale or sharing, or to limit the use of sensitive personal information. As already noted, the CCPA and CPRA already do not

provide many mechanisms to make it easier for consumers to exercise their rights. These changes further exacerbate this issue by requiring consumers to file even more requests to safeguard and exert control over their own information. Businesses, by the nature of the contractor or service provider relationship, have both a knowledge of which third parties they share information with, and a means of communicating with those third parties. Consumers have neither.

These changes will allow businesses to obscure how consumer information flows through any number of companies and make it significantly more difficult for consumers to exercise their rights under the CCPA and CPRA. It places a significantly greater burden on consumers who wish to safeguard their privacy. Indeed, the combination of being required to file duplicative requests with each separate entity and being kept in the dark about which companies control their data in the first place may make it impossible for many consumers to exercise their rights at all.

§ 7023. Requests to Correct.

In §7023, as elsewhere in the draft regulations, the Agency has potentially narrowed the instances in which a business must pass on requests—in this instance, to correct information, which raise concerns that businesses may leave uncorrected any information that is not specifically mentioned in a written contract, even if a consumer requests it be corrected. The draft regulations have also removed several illustrative examples from this section, which provided clear and valuable guidance about how this new right should be implemented.

We also do not understand the addition, in §7023(d)(1), of a requirement for consumers to make a "good-faith effort to provide businesses with all necessary information available at the time of the request." This provision will require more clarification for

consumers to be able to comply with it. As written, it could prevent consumers from being able to exercise this right at all. Consumers often will not know what kind of information a business may deem necessary to make a correction request.

We also would oppose any effort from business to raise this bar so high that no average consumer would be able to demonstrate a "good-faith" effort. Some businesses have already required processes that are far more rigorous than is necessary to comply with CCPA requests—such as requesting notarization or signing an affidavit to verify people's identities to fulfill requests.[8] As such, more specificity about what constitutes a "good-faith" effort would aid consumers in understanding their own obligations.

§ 7025. The Regulations Inappropriately Permit Dark Patterns when processing in a "nonfrictionless manner"

We have previously objected to the concept of permitted "non-frictionless processing" under section 7025(e), wherein businesses are expressly authorized to introduce any of the dark patterns outlined in 7004 - characterized as "friction" - when processing an opt-out preference signal, as long as they also include a "Do Not Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" link on the business's homepage.

This framework threatens to make the opt-out preference signals an unusable mechanism to communicate a consumer's privacy choices, with businesses able to rely on practices that this Agency acknowledges subvert user autonomy and has the effect of manipulating consumers. Interface interference and asymmetric choices with privacy-invasive options selected by default, coerced actions nagging users that have enabled opt-out preference signals, and pop-up text, graphic animation, sound and video content will be used

[8] Margaret Oates, *Identity verification: flows we've seen in CCPA data requests*, Consumer Reports (July 2022) https://digital-lab-wp.consumerreports.org/2022/07/07/identity-verification-flows-weve-seen-in-ccpa-data-requests-2-of-2/.

to discourage consumers from using opt-out preference signals. What should be a mechanism to seamlessly and frictionlessly communicate a consumer's right to exercise privacy choices will instead open up the consumer to the same kinds of abusive practices that are otherwise prohibited by the CCPA. Permitting this kind of mischief is inconsistent with both the explicit mandate of the statute, which does not permit dark patterns in response to opt-out preference signals, and the intent of the ballot initiative, which is to increase opt-out preference signal protections under California law.

Respectfully Submitted,

Emory Roane, Privacy Rights Clearinghouse

Halyley Tsukayama, Electronic Frontier Foundation

Becca Cramer-Mowder, ACLU California Action

Jacob Snow, ACLU California Action

Tracy Rosenberg, Oakland Privacy and Media Alliance

Susan Grant, Consumer Federation of America