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

to the

CALIFORNIA PRIVACY PROTECTION AGENCY
On Proposed Rulemaking Under the California Privacy Rights Act of 2020

(Proceeding No. 01-21)

August 23, 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.

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.

Access Humboldt is a non-profit, community media & broadband access organization serving the residents and local jurisdictions of Humboldt County on the North Coast of California USA, managing resources that include: streaming channel online; cable access TV channels; KZZH FM 96.7 community radio; media collection on Community Media Archive; a wide area broadband network with dedicated optic fiber connections to twenty locations serving local jurisdictions and community anchor institutions; broadband access wireless networks; a Community Media Center with studio and other production equipment and training on the College of the Redwoods campus; and ongoing operational support for public, educational and governmental access media services.

Consumer Action has been a champion of underrepresented consumers since 1971. A national, nonprofit 501(c)(3) organization, Consumer Action focuses on financial education that empowers low to moderate income and limited-English-speaking consumers to financially prosper. It also advocates for consumers in the media and before lawmakers and regulators to advance consumer rights and promote industry-wide change particularly in the fields of consumer protection, credit, banking, housing, privacy, insurance and utilities.

Data Minimization Language Rightly Centers Consumer Expectations in § 7002

Data minimization is a key tool for consumer protection, as it both ensures businesses are not over-collecting information and ensures that data collected from consumers aligns with their expectations. The Agency should set the standards for consumer rights based on consumer expectations—otherwise, such rules risk being counter to the goals of true data minimization. Establishing this frame ensures that consumers are not surprised by how their information is collected, used, or retained.

The proposed regulations language rightly establishes that the minimization standard should be "consistent with what an average consumer would expect when the personal information was collected." Similarly, it states clearly that if businesses seek to use information for another disclosed purpose, such purpose must be "compatible with what is reasonably expected by the average consumer."

We also appreciate the illustrative examples the Agency has outlined, which further clarify what consumers can expect in real-world applications that are easy for the average person to understand.

In particular, the example stating that a cloud-storage provider may not use personal information uploaded by a consumer to "improve cloud storage services" to "research and develop unrelated or unexpected new products or services, such as facial recognition…" without explicit consent. This is a clear and important marker to lay down in the name of consumer protection. Businesses are not the sole arbiters of what "improving" services may look like, and should have strictly limited latitude to repurpose information they have already collected for other purposes.

It is also good that the examples expressly say that businesses, such as internet service providers, that collect information to administer services, should not sell information to data brokers without a consumer's express consent. This makes clear that information is important to the consumer, and not merely another asset for a business to mark on a ledger.

While—to be most protective of consumer information—we would rather see businesses only collect information that is "necessary" or "strictly necessary" to the purposes consumers ask for, we understand that is not the standard set in current law. As such, the regulations clarify the statutory language in a way that protects consumers. Company expectations should not be the yardstick by which we measure what a related purpose may be. The proposed regulations recognize that consumer expectations should be the yardstick.

Dark Patterns Language in § 7004

We supported the proposed regulations from the California Department of Justice (DOJ) to protect against deceptive or coercive design choices, which are commonly called "dark patterns," in their proposal published October 12, 2020—specifically at Section 999.315(h), within the third set of proposed modifications of CCPA regulations, which the California DOJ published on October 12. Specifically, these regulations:

Require opt-out processes to be "easy" and "require minimal steps."

Ban opt-out processes "designed with the purpose or having the substantial effect of subverting or impairing a consumer's choice to opt-out."

Limit the number of steps to opt-out to the number of steps to later opt back in.

Ban "confusing language" such as "double negatives" (like "don't not sell").

Ban the necessity to search or scroll through a document to find the opt-out button.

The Agency's proposed rules build on this foundation substantially by adding more detail and language responsive to how consumers are often asked to make privacy choices in the real world.

Not only must businesses make sure their instructions are easily understandable, they also must have symmetry in choice and make clear design choices. This is important to specify in regulations, as companies too often seek to confuse or even shame people into making a decision that works against their own privacy interests or preferences. It is also important for these regulations to state that exercising one's privacy rights should not be limited by unnecessary bureaucratic or administrative steps.

The Draft Regulations Inappropriately Introduce "Frictionless" and "Non-Frictionless" Processing of Opt-Out Preference Signals in § 7025(e)

Opt-out preference signals allow consumers to easily exercise their privacy choices by configuring a single setting that automatically expresses that privacy choice when they visit a business's website or use an app. This mechanism was present in the California Consumer Privacy Act (CCPA) regulations issued by then-Attorney General Becerra and was reinforced in the California Privacy Rights Act (CPRA) supported by a majority of California voters later that year.[1]

Proposition 24 changes the legal relationship between opt-out preference signals and the requirements to include prominently placed "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links on the business's website.[2]

[1] 11 CCR § 7026(a); *see also* Cal. Civ. Code §1798.135(b)
[2] Cal. Civ. Code §1798.135(b)(1),(3).

The Draft Regulations state in Section 7025(e), "Civil Code section 1798.135, subdivisions (b)(1) and (3) provides a business the choice"; a business can process opt-out preference signals in a "frictionless manner" or the business can elect to include those conspicuously placed links and are then permitted to process opt-out preference signals in a "non-frictionless manner."[3] The draft regulations later describe what is permitted when businesses process opt-out preference signals in a "non-frictionless manner" by defining a "frictionless" processing in section 7025(f) as prohibiting: (1) charging a fee or requiring valuable consideration if the consumer uses an opt-out preference signal, (2) changing the consumer's experience with the product or service, or (3) displaying a notification, pop-up, text, graphic, sound, video, "or any interstitial content" in response to an opt-out preference signal.[4]

"Non-frictionless" is not defined, but the draft regulations suggest that the "friction" could include all of these consumer-hostile tactics: charging consumers a fee, degrading their service or experience, and badgering them with pop-ups, videos, and other interstitial content.

The concepts of "frictionless" and "non-frictionless" processing are not present in the CCPA, its current implementing regulations, or the CPRA. In creating these categories, the Agency risks enshrining in regulation discriminatory and harmful business practices.

By implicitly validating "non-frictionless" processing of an opt-out preference signal, the regulations threaten to open the floodgates of deceptive and manipulative design from companies who will take every opportunity to deprive consumers of their privacy and their ability to make simple choices to protect themselves.

[3] Draft Regulations § 7025(e)
[4] Draft Regulations §7025(f)

We oppose this proposed framework and recommend striking the concept "non-frictionless processing" from the draft regulations. When a business processes an opt-out preference signal, that processing must be done in a manner that comports with the requirements and principles outlined in the law. Businesses cannot be permitted to markedly degrade the consumer experience of those using opt-out preference signals simply because the business elected to include conspicuous privacy links on their homepage and privacy policy.

"Non-frictionless" Processing in 7025(e) Authorizes Privacy Dark Patterns.

In addition, permitting businesses to interpret opt-out signals in a "non-frictionless" manner would invite the very same dark patterns that the draft regulations aim to prohibit. A business that posts the necessary conspicuous links is not subject to the prohibitions in § 7025(f). As a result, under the regulations, businesses could apparently add popups or interstitial graphics responding to a user's opt-out signal. These popups could prompt the user that the business will charge the user a fee to continue using the website with their opt-out signal still enabled. And even after the user gets past the pop-ups, they could be redirected to a site that is different than one for a user without an opt-out signal enabled.

This user experience is not in the letter or the spirit of § 7004. This section gives us the five principles for obtaining user consent and outlines what may constitute a dark pattern. In § 7004(a)(2), the Symmetry in Choice principle states that "the path for a consumer to exercise a more privacy-protective option shall not be longer than the path to exercise a less privacy-protective option." However, a business adding friction after recognizing an opt-out signal is not symmetrical in choice because it would make the path to a website longer for someone with an opt-out signal enabled.

Even the double-negative phrase “non-frictionless” violates the regulations caution in § 7004(a)(3) to “[a]void language or interactive elements that are confusing to the consumer,” which notes in particular, “the methods should not use double negatives.”

Further, § 7004(a)(5) states that CCPA requests should be easy to execute, and that businesses shall not add unnecessary burden or friction. However, § 7025(e) says exactly the opposite, that businesses can add friction when responding to an opt-out signal if they are authorized to do so in a “non-frictionless manner.” Finally, § 7004(c) states that a dark pattern is an interface that "has the effect of substantially subverting or impairing user autonomy, decision-making, or choice." A user with an opt-out signal has expressed a clear intent to exercise their privacy rights. Adding friction to that process that has the effect of substantially subverting the user’s intent is a dark pattern.

For this reason and the others listed, we object to the inclusion of a “non-frictionless” form of permitted processing, which would have the effect of undermining the intent and purpose of opt-out preference signals and validate dark patterns as an approved business practice.

Definition of Disproportionate Effort in § 7001 (h)

We are concerned that the definition of disproportionate effort added to § 7001 (h) allows the projected benefit to the consumer to be completely defined by the business rather than by the consumer. This is an especially acute issue when the personal information in question is sensitive information as defined by the statute.

If inaccurate data causes a consumer to miss a business opportunity, be denied a loan or a job, the consequences or damages experienced by the consumer may be exceptionally high, if not

fundamentally unlimited, and it isn't clear that a business would be aware of, or able to accurately measure, the benefit to the consumer or the potential lifelong ramifications.

The model also sets up a power dynamic that allows the business to set the terms of the projected benefit to the consumer as measured against their own effort. We question whether having businesses "tell people" how much they benefit is consistent with the overall intention of CCPA and CPRA to put consumers in the driver's seat regarding how their personal information is handled.

We recommend that, at a minimum, the Agency consider whether setting some floors on the minimum amount of effort that can be claimed to be disproportionate to a consumer's benefit and that such a floor may not be the same for sensitive data as for non-sensitive data. Similarly, the process of using a disproportionate effort claim to refuse a consumer request should have an input mechanism for a consumer to understand the business' interpretation of the benefit to them and to add additional information if needed to understand the true nature of their request.

That said, it remains unclear to us what happens if 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, and the consumer disagrees with that assessment by the business.

Financial Incentives in §7016

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 not to participate.

The potential dangers of widespread Pay-For-Privacy programs is that affluent consumers will retain the full ability to opt-in or opt-out as they choose, and less affluent consumers will be unable to afford the increased costs incurred by a choice to opt-out. We encourage the Agency to keep this dystopian scenario in mind as businesses move into full compliance with CCPA/CPRA and be prepared for further rulemaking within the limits of the statutory language to protect the rights of consumers without financial means to fully use the privacy rights granted to them without excessive financial punishment.

Pay-for-Privacy programs can range from the benign (one free latte after buying ten at your favorite coffee house) to the considerably less so: for example, Amazon's $10 per palm print offer which trades checkout speed at Amazon Go outlets for the dubious benefit of building out a biometric database for the gigantic online retailer with its many ties to law enforcement.[5]

We were disappointed to see the draft regulations by the Agency leave mostly untouched the extreme license given to businesses to compute "the value of the customer's data" according to seemingly almost any formula or method that they choose. The lack of specific guidance will likely result in a crazy-quilt assortment of methods that will be used 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 neither the statute itself nor these regulations provide a standard to ensure that the value number itself is reasonable. For a financial incentive to be reasonably related to an unreasonable value computation seems neither reasonable nor protective to consumers.

[5] *See* https://techcrunch.com/2021/08/02/amazon-credit-palm-biometrics/

This section of the statute is in tension with the data minimization precepts in other parts of the law. This tension is perhaps accentuated by the strong data minimization language the Agency proposed adding in these draft regulations. If no data is to be collected other than what a reasonable customer would expect is needed to provide the service and product the consumer has requested, then the value of the data to the business is, by definition, somewhat constrained.

To cite the example provided above, Amazon has assigned a financial incentive of $10 to the opt-in acquisition of a biometric palm print to aid in rapid check-out at Amazon Go locations. The figure of $10 is thus nominally "reasonably related" to the value of the biometric palm print to Amazon. But what does these $10 (or thereabouts) value to Amazon consist of? Does it really benefit Amazon at a rate of $10 per consumer to check a customer out of their store with a palm print instead of a scan of a debit or credit card? Certainly, there may be some labor savings, but they could not add up to $10 per customer. The value is connected to the acquisition of the palm print for other business purposes besides checking out of Amazon Go stores, which then demands the question of whether those other business purposes are consistent with what a reasonable customer would expect.

We recommend 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. The 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.

Amendment Provision of CPRA

We additionally suggest the Agency create specific language to govern the future of privacy legislation more clearly in California. The ballot initiative language of "in furtherance of privacy" is very general, and we have already seen significant questions arise over various legislative proposals by the Legislature. We can only assume that will be exacerbated in coming years; especially as innovative technologies stretch existing privacy definitions. The Legislature has already passed some legislation that we are dubious met the standard of "in furtherance of privacy", for example AB 335 in 2021.[6]

Supplemental language that addresses specifically empowering consumers to have more control over the handling of their personal information might provide a clearer frame for what kinds of legislation are included in the "furtherance of privacy" and what kinds are not. The Legislature will want and deserves some level of discretion, but the bottom line is that CPRA was a ballot initiative that promised voters that the privacy protections they were voting for could not be weakened or watered down. It is incumbent on the Agency to make sure that promise is kept.

s/

Hayley Tsukayama, Electronic Frontier Foundation

Becca Cramer-Mowder, ACLU California Action

Jacob Snow, ACLU California Action

Emory Roane, Privacy Rights Clearinghouse

[6] *See* https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202120220AB335

Tracy Rosenberg, Oakland Privacy and Media Alliance

Susan Grant, Consumer Federation of America

Sean Taketa McLaughlin, Access Humboldt

Ruth Susswein, Consumer Action