Santa Clara University

Comments to the CPPA's Proposed Regulations
Pursuant to the Consumer Privacy Rights Act of 2020

August 23, 2022

Brian Soublet
The California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834
By email: regulations@cppa.ca.gov

I am a tenured law professor at Santa Clara University School of Law, where I teach Internet Law and direct the school's Privacy Law Certificate. These comments represent only my views and not the views of my employer or any third party.

Section	Proposed Revisions	Explanation
7001(h)	1) Change "significantly outweighs" to "outweighs" 2) Change "the benefit provided to the consumer" to "the benefit to the consumer (as documented by credible evidence from the consumer)" 3) Add "A business need not consider any consumer benefit that is not documented by credible evidence or is obviously pretextual." 4) Delete everything after the first sentence. If not, make corresponding changes and define "adequate."	Asking businesses to evaluate consumers' benefits does not work. Businesses rarely know or can confidently guess what benefits consumers will idiosyncratically derive, and consumer self-reports of their purported "benefits" are unreliable and easily gamed. Instead of adopting my suggestions, a better approach would be to adopt a definition that doesn't depend on gauging consumer benefit at all.

Section	Proposed Revisions	Explanation
7002(a) 7002(b) 7027(a) 7027(l) 7053(a)	Replace "average" consumer with "reasonable" consumer	The CADOJ proposed the "average consumer" phrase in its initial draft of the CCPA regulations, but then it backtracked when it recognized the error of its ways. It's unfortunate that this phrase has been resurrected. As I wrote in response to the initial regulations: "The 'average consumer' standard does not represent the prevailing national approach in consumer protection law. The FTC expressly considered the appropriate standard for measuring consumer confusion in its 1983 Policy Statement on Deception. In that statement, the FTC adopted the standard of 'a consumer acting reasonably in the circumstances.' This standard has served consumers and the FTC well for over three decades. Among other advantages, it avoids the indeterminacy of defining what constitutes an 'average' consumer when a business caters to multiple heterogeneous consumer segments."
7003(c)	Replace "other" with "the smallest text-based"	Websites contain links in a variety of formats (such as text, images, and buttons) and sizes. The proposed regulation incorrectly assumes a single standard for how links are presented.
7004(a)(2)	1) Replace "symmetry" with "similarity" 2) Replace "shall not be longer" with "shall not require consumers to take more steps or actions" 3) In subpart (D), delete "more prominent (i.e.," the end parenthesis, and "is not symmetrical"	"Symmetry" implies "equality," but it's impossible to promote two items "equally" on a web page. By definition, one option must always be to the left of, or above, other options. Subpart (D) similarly assumes that options can have equal prominence.

Section	Proposed Revisions	Explanation
7004(a)(4)	1) Define "choice architecture" 2) Delete the "guilt or shame" and "manipulative and shaming" standard 3) Define "bundles consent"	The terms "choice architecture" and "bundled consent" are jargon. The proposed restrictions on "guilting" and "shaming" are improper. Businesses cannot control or always anticipate consumers' subjective feelings. Furthermore, all persuasive material, including advertising, necessarily prompts consumers to think about and second-guess their choices. The regulation essentially equates standard marketing techniques with "guilting" or "shaming" techniques. Thus, the proposed standard is both indeterminate on the businesses' side and overinclusive on the enforcement side. Standard false advertising principles of deception and unfairness can sufficiently police any abusive business practices in this situation.
7004(a)(5)	1) Define "unnecessary burden or friction" 2) Define "aggressive filters" 3) Define "unnecessarily wait"	These terms are jargon.
7004(b)	Reconsider the definition of "dark pattern" and possibly define "user interfaces"	The CPRA authorizes the CPPA to define "dark patterns" only with respect to "user interfaces." The statute does not define "user interface," but typically the term includes only actual "interfaces," not every aspect of a business' goods/service or operations. Parts of 7004(a) seem likely to reach beyond "user interfaces," such as restrictions on a product's "choice architecture" (whatever that jargon means). The CPPA should reevaluate if its definition of "dark patterns" stays within the scope of its authority. It may also be worth defining "user interface" to self-impose boundaries on the scope of dark patterns.

Section	Proposed Revisions	Explanation
7012(f)	Delete the last sentence	Deep-linking is not always possible due to technological constraints. The requirement also assumes that a disclosure will fully address the applicable topic in a single place, but consumers often need to read the entire disclosure (including definitions, disclaimers, exceptions, and more) to properly understand any specific provision. In those cases, deeplinking will hinder consumer understanding. Also, businesses do not control the displays on consumers' devices, so scrolling may be required even if a business uses deeplinking.
7015(b)	Replace "any other" with "the smallest"	Businesses will use many different-sized icons on their website. It would not be proper to require businesses to make this opt-out icon as large as the largest icon on the page. That would clutter up pages, would not be scalable if other regulators took the same position, and would disrupt the businesses' abilities to maximize the page's helpfulness to consumers.

Section	Proposed Revisions	Explanation
7023	1) In (b), replace "determines that the contested personal information is more likely than not accurate based on the totality of the circumstances" with "has a reason to believe that the requested correction may not be accurate" 2) Delete (b)(2) 3) Delete (d)(2)(D) or make changes similar to those mentioned in 7001(h) 4) In part (f), add an immunity for the explanations 5) In part (f), add a qualifier that businesses are required to append information to a record only when their database software is designed to accommodate that function. 6) In part (f), add the following: "No explanations are required where disclosures would expose trade secrets, put the business at a competitive disadvantage, or increase the business' risk of exposure to consumers' attempts to undermine its policies or offerings." 7) Similar qualifications should be made to part (i). 8) In part (g), delete "within the past six months of receiving the request."	The proposed correction process does not follow good information governance practices. It requires businesses to "adjudicate" the truth of disputed information—but skews the businesses' incentives towards accepting the consumer's assertions even when the consumer may be wrong or lying. Thus, the proposed regulation facilitates the collection and propagation of inaccurate information. The proposed regulation stacks the decks in favor of inaccurate information. First, it says the business must accept the correction even if it has 49% doubt about the veracity. Second, it puts the burden on businesses to document and explain why they think a consumer's correction request is fraudulent or abusive. Together, these burdens (and the associated legal risk) pushes businesses towards acquiescing to consumer correction requests, even when the business has substantial doubts about the correction's veracity. When consumers manipulate these burdens to force improper corrections, it harms everyone. The corrected information will be relied upon by other businesses, and consumers can weaponize the undeserved trust in data quality to commit fraud or perpetrate public deceptions. This also puts the business at risk of legal liability if they are sharing false information that consumers forced into their databases. The explanations requirement further nudges businesses towards accepting improper corrections. By definition, this issue will arise only when the facts are contested, which means the businesses are already unsure of what's the "truth." Then, if businesses reject the correction, they will fear liability for whatever they disclose in the explanations (*see, e.g.*, Isaac v. Twitter, Inc., 557 F. Supp. 3d 1251 (S.D. Fla. 2021))—another liability risk they can avoid by acquiescing. To avoid the pro-inaccuracy implications of the explanations liability, the

		regulations should provide an immunity from liability for these disclosures. Explanations may also enable consumers to engage in adversarial behavior, such as gaming the business' policies/systems or exposing trade secrets. Explanations should not be required where those consequences are possible. Appending information to records should be required only when a business' database software facilitates it. Otherwise, this requirement may impose disproportionate costs on businesses because they will have to change databases to accommodate the requirement. Part (d)(2)(D) makes the same error as 7001(h). Businesses cannot assess the idiosyncratic impacts on consumers unless the impact has been credibly documented to them. Part (g) seems to authorize a consumer to reargue the exact same issue 2x/year in perpetuity, with all of the associated costs. That doesn't serve anyone's interests.

Section	Proposed Revisions	Explanation
7025	Add a certification process before any technology is legally designated as an opt-out preference signal, and add a phase-in period for businesses to accommodate the designation	As ridiculous as it was for the California Attorney General to tweet that the CADOJ considered the Global Privacy Control to be a qualifying opt-out signal, the tweet at least provided guidance to the business community about the department's views. Without that tweet, businesses would otherwise have to guess what technologies qualify because the regulations do not provide any other official signals to businesses. The CPPA should develop a process for validating software that meets the regulatory standards, publicize its determination to the community, and give businesses an adequate period to make the technical adjustments on their side. Even tweets from the CPPA would be more helpful than the current proposed regulation.
7025(g)(2)	Delete part (C)	This provision has unintended consequences. Effectively, it requires a business to encourage consumers to adopt opt-out preference signals to communicate directly with it, but the consumer's adoption of an opt-out preference signal will affect the consumer's relationships with all businesses, not just the one business in question. In other words, a consumer's decision to adopt an opt-out preference signal just to interact with one business will have a much broader and potentially unwanted and unanticipatable effects. The proposed regulation implicitly encourages consumers to make this consequential choice with incomplete information.
7060(b)	Delete	The regulations proceed on the assumption that opt-outs or requests to limits will always be in the consumers' interests, but in fact they are weaponizable by adversaries like the other CPRA's consumer rights. Thus, these requests should be authenticated as well.
7062(d)	Delete "or correction of the spelling of a name"	Name corrections are a vector of attack for identity theft.

Section	Proposed Revisions	Explanation
7102	Delete	If the CPPA wants to continue this non-statutory requirement, it should provide empirical justification that the transparency reports benefit anyone. I am unaware of any such empirical support. The initial statements of reasons makes an unsupported empirical claim that the disclosures are "necessary to inform the Agency, Attorney General, policymakers, academics, and members of the public about businesses' compliance with the CCPA." I trust the Agency would make that empirical claim only if it had substantial evidence demonstrating that necessity based on actual in-the-field data since the existing requirement has been in effect. Many people, including me, would like to see the Agency's supporting evidence. Until then, the public evidence to date vitiates the purported "necessity" because the initial batch of transparency reports appeared to be useless. *See, e.g.* Susannah Luthi, *'Functionally Useless': California Privacy Law's Big Reveal Falls Short*, POLITICO (Aug. 5, 2021). The likely failure of these disclosures aren't surprising; there is an extensive literature on why mandatory disclosures fail. *E.g.* ARCHON FUNG, MARY GRAHAM & DAVID WEIL, FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY (2007); OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE (2014). Failure is virtually guaranteed when a regulator doesn't follow best practices in structuring mandatory disclosure requirements (which the CADOJ did not do). Until it can provide empirical proof of the purported "necessity," the CPPA should abandon this section as a failed regulatory experiment.

Section	Proposed Revisions	Explanation
7304	Add a requirement that any audit is authorized only when the Agency complies with applicable legal process	The CPPA has a wide range of investigatory tools available to it, including information demands, administrative subpoenas, and court orders. The regulations should specify that any "audit" is permitted only after the CPPA has followed the appropriate legal process associated with the information the CPPA seeks to obtain. Any lesser standard exceeds the CPPA's legal authority and raises major constitutional problems. With respect to ensuring recidivist noncompliance, the CPPA can include audit rights in any settlement or consent order. No regulation is required to implement that.

Two other points beyond the proposed regulations:

First, the CPPA has already missed its statutory deadline for completing the rule-making process, and this delay ensures that businesses will not get an appropriate and fair turnaround time to implement the regulations. The CPPA should provide explicit guidance on an updated schedule for businesses' expected compliance obligations and the CPPA's enforcement efforts.

Second, the statement of financial impact raises several red flags about how the CPPA is justifying its regulations, including:

- The supporting economic report (which did not include the authoring firm's name, a perhaps prudent decision given its problems) excluded businesses that are GDPR-"compliant" from its calculations.[*] Why? The CPPA's Notice of Proposed Rulemaking expressly acknowledges "key differences between the GDPR and CCPA, especially in terms of how personal information is defined and the consumer's right to opt-out of the sale or sharing of personal information (which is not required in the GDPR)." Given the CPPA's position about the dissimilarities of the CCPA and GDPR, it is contradictory for the CPPA's economic report to treat GDPR "compliance" as part of the regulatory baseline. Indeed, it raises questions about how the CPPA could accept the report with such a critical (and obvious) conflict with the CPPA's own positions.
- Section B(3) of the statement of financial impact estimates that reporting businesses will incur $2.8M in annual compliance costs. Yet, the statement of financial impact also estimates lifetime compliance with the regulations will cost $8M total. The CPPA should explain these apparent discrepancies.
- The economic report's estimate that it will take businesses 1.5 hours of compliance with the new regulations is not credible. It's not possible to read and understand the 29,000+

[*] I do not know any privacy practitioner who would say that a company can be GDPR-"compliant" due to the ongoing and indeterminate nature of the GDPR's requirements.

words in the proposed regulations in 1.5 hours,[**] let alone actually interpret them, make judgments about which regulations require changes, and then implement those changes. As just one of dozens of possible unaccounted-for costs, businesses may need new software to accommodate the correction appending requirements, with associated (and potentially substantial) acquisition, migration, and training costs. I do not understand how the economic consultant failed to model that scenario. The failure to properly account for the true economic consequences of the proposed regulations raises obvious questions about whether this rule-making process complies with California law.

Thank you for considering my comments.

Professor Eric Goldman
Associate Dean for Research
Co-Director, High Tech Law Institute
Supervisor, Privacy Law Certificate
Santa Clara University School of Law
500 El Camino Real
Santa Clara, CA 95053
408-554-4369
egoldman@gmail.com
http://www.ericgoldman.org
http://twitter.com/ericgoldman

[**] If a reader could maintain an average reading speed of 250 words per minute, the regulations would take about 2 hours to read.