Script

Good morning. I'm Noreen Whysel, Director of Validation Research at the Me2B Alliance. I should note that today we've changed our name to Internet Safety Labs. We are a non-profit product safety testing organization for connected technology. I lead qualitative research to understand people's experiences and relationships with the technology they use.

I am a professor in Communication Design at CUNY's New York City College of Technology and have written and presented research on dark patterns, accessibility, and vulnerable populations.

Up front, I would like to present our recommendations regarding CPRA and "Dark Patterns" and then describe them further during this time.

1. As others mentioned, stop using the term "Dark Patterns." Focus on the harmful outcomes of these interfaces by calling them what they are "Harmful UI Patterns."
2. "Opt-Out" should be the default condition, not a choice. That's a big one for us.
3. Adopt a framework for identifying Harmful UI Patterns at each stage of a technology relationship.
4. We also have specific recommendations about the definitions of "Consent" and "Intentional Interaction" which I'll describe.

1. "Dark Patterns"

In CPRA, the definition of "Dark pattern" affirms that designers are responsible for the effects of the UI pattern that causes harm. The outcome of the interaction is important. We state in our Me2B Rules of Engagement that technologies should not willfully harm their users, but there is a willful neglect in adopting UI patterns just because they are easy, or because they are embedded in the systems we use to design a product.

That said, I'd like to use my time to focus on the outcome of these "Harmful UI Patterns." Notice I didn't say "Dark." Industry is re-defining so-called "dark patterns" as "deceptive patterns" and California should follow suit. Last month, Harry Brignull, the British ethicist, well-known to have coined the "dark patterns" phrase, changed his darkpatterns.org website name and URL to "deceptive.design" following a trend championed by organizations such as the Web Foundation's Tech Policy Design Lab who represent the new label as more inclusive.

In fact, we at the Me2B Alliance prefer the term "Harmful UI Pattern" as it describes the outcome of the design pattern that affects the individual agency of the technology consumer.

We know from our research that people understand that they are being treated unfairly and that they know that good UI patterns use clear and specific language so they can make decisions without feeling coerced.

2. Opt Out versus Opt In

The reliance on “Opt-Out” from data sharing as a choice requires a user action to be effected. This opens the door to harmful UI patterns. We support the practice of easy to use, Opt-In methods with Opt-Out set as the default.

Requiring people to Opt Out is one of the Harmful UI Patterns frequently cited in literature, in Harry Brignull ‘s research, and is further defined in a “dark pattern” taxonomy developed by Purdue University’s User Experience Pedagogy and Practice Lab (UXP2) (funded by National Science Foundation Grant #1657310). According to Purdue, “the use of checkboxes to opt out rather than opt in....” is listed and categorized as “Interface Interference.”

Requiring Opt Out, whether paired with confusing wording or not, creates an asymmetrical power dynamic leading to harmful levels of data sharing and surveillance tracking and to a disruption of agency in people who use connected technology. It does not promote the safety and wellbeing of people and is not harmonized with global norms.

In addition, we should not assume people know that they need to Opt Out. Instead, allow people the agency to decide whether to Opt In.

3. A Framework for Identifying Harmful UI Patterns

- We recommend that the regulation include or reference additional examples of Harmful UI Patterns, and identify a framework for when they are likely to occur

A framework for identifying Harmful UI Patterns would be helpful, especially given that many potentially Harmful UI Patterns have yet to be designed. It would help designers to understand when they occur and what harms they cause.

Harmful UI Patterns exist along the spectrum of the entire technology relationship, beginning before an account or other user relationship is established until well after it’s terminated. I emphasize this because people don’t always know that these UI patterns can exist before the traditional onboarding stages or after account termination.

To provide clarity, the Me2B Alliance has identified what we call a Me2B Relationship Lifecycle, or transactional stages that occur during technology use over time where consent to various actions occur. These commitments map to the stages of social interactions as defined by George Levenger: Acquaintance, Buildup, Marriage, Deterioration and Termination.

In each of these stages, there is a potential for introducing Harmful UI Patterns and negative UX Outcomes, such as:

- In the initial acquaintance stage, harmful patterns might include making it difficult to view content without creating an account, sharing personal contacts, or entering a credit card number.

- In the buildup or onboarding stage: requiring access to contacts or location information when signing up for newsletters, notifications, or loyalty programs when use of these data aren't necessary or legitimate.
- Long, convoluted, and Nagging processes for closing an account or reducing any other levels of commitment.
- And requiring Opt Out or requiring people to deselect Opt In at any stage.

The establishment of each commitment may not be obvious to users. But in what we call the Invisible Parallel Dataverse data is collected and shared with third parties and the temptation to use deceptive or harmful UI patterns to accelerate data collection at each commitment stage is a risk. These patterns are frustrating and can encourage people to simply stop using the service without closing an account, which preserves data sharing settings in perpetuity, another example of the unequal power dynamic between technology and user.

4. Definitions of "Consent" and "Intentional Interaction":

The "Consent" definition should use "harmful UI pattern" instead of "dark pattern."

And in the "Intentional Interaction" definition, note that opening a website does not necessarily mean there is an intention as so many harmful UI patterns are designed to get you to load something on your device that you didn't intend. We've all done this. We would recommend adding a statement to the "Intentional Interaction" definition, similar to the one in the "Consent" definition that says: "***Likewise, user behaviors that occur through use of Harmful UI Patterns do not constitute an intent to interact."***

And in the subsection on privacy policies, where it mentions avoiding technical and legal jargon, it should note the reason for this is that complex language is a harmful UI pattern. We would go further to describe tests for readability and understandability, as defined by W3C WCAG 2.1 and described in our recently released Me2B Safe Specification, which includes readability and understandability tests based on standards for reading levels and cognitive ability.

In sum:

The regulation's definition of exactly what UX Designs will constitute a harmful UI pattern remains unclear and requires specific guidelines. It starts with using language that aligns with global norms: Harmful patterns, not "dark patterns" and ensuring that the user experience outcome is the focus. Providing examples of Harmful UI Patterns that are typical at each commitment stage of a technology relationship, would be helpful in defining when a pattern is harmful. Our Me2B Safe Specification could be helpful as it describes each technology commitment in detail and provides UI tests for violations of rules around clear notice, accessible language, and the minimization of data collection.

Thank you

Thank you for the opportunity to share our thoughts about what we should be calling “harmful UI patterns.” It has been an honor to participate in this important legislation.

End Script

OLD Script

Good Morning. My name is Noreen Whysel and I am the Director of Validation Research at the Me2B Alliance. I should note that we’ve changed our name to Internet Safety Labs. We are a non-profit product safety testing organization for connected technology. I lead qualitative research to understand people’s experiences and relationships with the technology they use. Our research informs and validates requirements for safe and respectful technology behaviors that are outlined in the recently published Me2B Safe Specification.

In addition to my work at the Me2B Alliance, I am an adjunct lecturer in UX and Communication Design at CUNY’s New York City College of Technology and have published research and presented at industry conferences on dark patterns, accessibility and vulnerable populations. I participate as a UX and accessibility expert in working groups for the Kantara Initiative and the W3C.

What follows are our comments and recommendations regarding CPRA and “Dark Patterns”.

In CPRA, the definition of “Dark pattern” affirms that designers are responsible for the effects of the UI pattern that causes harms, which is something that many UX designers recognize as a core responsibility. The user experience outcome is important in determining whether there is harm. While we state in our Me2B Rules of Engagement that technologies should not willfully harm its users, there is a kind of willful neglect in adopting UI patterns just because they are easy, or because they are embedded in the system we use to design a product.

That said, I’d like to use my time to focus on harms as an outcome of Dark Patterns.

As an illustration of the effects of these harms, I thought I’d start with some quotations from recent research about how people view their relationship with technology. Our research participants described technology behaviors that coerce and manipulate them. They describe these behaviors as “Creepy” and feel powerless to regain any sense of control. One said, and I quote:

> “I always just considered it a given that companies [are] sucking up my information no matter what. And that's why I have to agree to those terms and conditions or the privacy policy.”
> And when this happens? She says:
> “[T]he damage is done. They already violated my privacy … My data is already out there. So, what good would what I do now matter?”
> She even offered a solution:

> "Maybe [companies] should have a requirement that they write the terms and conditions in understandable, specific language. You know, like, 'we will not share?'" She suggested, "They [should] say in the terms and conditions - real succinctly - What they're doing. [What they are] [p]laying at. You know, rather than make it so long and complicated. Nobody reads it, you know."

CPRA appears to agree. In **§ 999.308 on Privacy Policy,** it states "the privacy policy shall be designed and presented in a way that is *easy to read* and *understandable* to consumers. I'd go further to describe tests for readability and understandability, as defined by W3C WCAG 2.1 and described in our recently released Me2B Safe Specification. This section should also state that a reason to avoid technical and legal jargon is that this language can be used as cover for Harmful UI Patterns.

You may notice that I didn't say "Dark Patterns." Industry is re-defining so-called "dark patterns" as "deceptive patterns." Harry Brignull, the British ethicist, well-known to have coined the "dark patterns" phrase, hosts a website at darkpatterns.org. Just this April, he changed his website name and URL to "deceptive.design" following a trend championed by organizations such as the Web Foundation's Tech Policy Design Lab , which moves away from labeling harmful UI patterns as "dark" toward refering them as "deceptive patterns."

The "deceptive patterns" label is less harmful and more inclusive. In fact, we at the Me2B Alliance prefer the term "Harmful UI Pattern" as it describes the outcome of the design pattern that affects the individual agency of the technology consumer. "Deceptive" or "Harmful" patterns hurt people. They cause emotional pain and psychological harm, in addition to the negative social and financial outcomes of surveillance, unwanted data sharing, and fraud that can be disguised as "user choice."

This leads to another issue with the legislation: In **§ 999.315. Requests to Opt-Out. (h) 1-5.** The reliance on "Opt-Out" from data sharing as a choice requires a user action to be effected. Why isn't "Opt-Out" the default condition? Requiring people to Opt Out is itself a Harmful UI Pattern. It favors the advertising and marketing industry, and does not promote the safety and wellbeing of people and isn't harmonized with global norms. Instead, we support the practice of easy to use, Opt-In methods.

Requiring users to opt out of data sharing is one of the Harmful UI Patterns frequently cited in literature, in Harry Brignull 's research, and is further defined in a "dark pattern" taxonomy developed by Purdue University (funded by National Science Foundation Grant #1657310). According to Purdue's User Experience Pedagogy and Practice Lab (UXP2), requiring a check box is listed and categorized as "Interface Interference" and states that "One common example of this tactic is the use of checkboxes to opt out rather than opt in...."

It is well documented, and as noted in the quote previously, well understood, that people rarely read terms of use, and that these documents lock people into an asymmetrical power dynamic leading to harmful levels of data sharing and surveillance tracking. Requiring Opt Out, whether paired with confusing wording or not, leads to a disruption of agency in people who use

connected technology, because they may not know what they opted into or even that they opted into something in the first place. As I've noted respectful default is Opt Out. Data sharing and surveillance tracking should never be the default state. We should not assume people know that they need to Opt Out. Instead, allow people the agency to decide whether to Opt In.

Another example of harmful patterns in the regulation is in the definition of "Intentional Interaction." The definition provides examples of interactions that may or may not trigger consent. It does not mention "dark patterns" but appears to suggest that certain user actions cannot be interpreted as consent, such as hovering, clicking or scrolling. We agree. We would also point out that the act of launching a web site should not be considered an intention to interact, as the definition seems to suggest it is. People accidentally open websites all the time whether by harmful UI patterns or by mistake. Consider including a statement in the Intentional Interaction definition like the one in the "Consent" definition: "***Likewise, user behaviors that occur through use of (I would say) Harmful UI Patterns do not constitute an intent to interact."*** Also, the "Consent" definition should use "harmful UI pattern" instead of "dark pattern."

The regulation should include or reference additional examples of Harmful UI Patterns, understanding that many potentially Harmful UI Patterns have yet to be designed. Harmful UI Patterns exist along the spectrum of the entire technology relationship, beginning before an account or other user relationship is established until well after it's terminated (if it's terminated). I emphasize this because people don't always know that these UI patterns can exist before the traditional onboarding stages or after account termination.

To provide clarity, the Me2B Alliance has identified what we describe as commitments, or transactional stages that occur during technology use over time, they map to the stages of social interactions as defined by George Levenger: Acquaintance, Buildup, Marriage, Deterioration and Termination. Many interactions or transactions can happen at each stage. In the onboarding phase from Acquaintance to Marriage phases, you visit a website, permit location tracking, sign up for a newsletter or phone notifications, create a user account, join a loyalty program, share content with a friend. In Deterioriation, perhaps you begin to turn off permissions, unsubscribe from newsletters, and in Termination, you may close your account or simply stop visiting.

In each of these stages, there is a potential for introducing Harmful UI Patterns and negative UX Outcomes, such as:

- Making it difficult to view content without creating an account, sharing personal contacts, or entering a credit card number.
- Requiring Opt Out or requiring people to deselect Opt In when signing up for a newsletter.
- Long, convoluted, and Nagging processes for closing an account or reducing any other levels of commitment. These in particular can encourage people to simply stop using the

service without closing an account, thus preserving data sharing settings in perpetuity, which may be a revenue goal for the technology and its data sharing partners. Another example of the unequal power dynamic between technology and user.

The establishment of each commitment may not be obvious to users. But in what we call the Invisible Parallel Dataverse data is collected and shared with third parties and the temptation to use deceptive or harmful UI patterns to accelerate data collection at each commitment stage is a risk.

In sum:

The regulation's definition of exactly what UX Designs will constitute a dark or harmful UI pattern remains unclear and requires specific guidelines. Providing examples of Harmful UI Patterns that are typical at each commitment stage of a technology relationship, would be helpful in defining when a pattern is harmful. Our Me2B Safe Specification describes each technology commitment in detail and provides UI tests for violations of rules around clear notice, accessible language, and the minimization of data collection.

Thank you for the opportunity to share our thoughts about "dark patterns". It has been an honor to participate in this important legislation.

End Script

Summary of recommendations:

- Change the "Dark Patterns" to terminology that aligns with industry trends toward more inclusive language. We prefer "Harmful UI Patterns" as it focuses on the UX Outcome. "Deceptive Pattern" or "Deceptive Design" are other phrases that are replacing the phrase "Dark Patterns."
- Change the "Consent" definition to reference "harmful UI patterns" instead of "dark patterns"
- Include a reference to Harmful UI Patterns in the definition of "Intentionally Interacts." since unintentional interactions are often triggered by Harmful UI Patterns. Consider including a statement in the Intentional Interaction definition such as the one in the "Consent" definition by appending it with: "***Likewise, user behaviors that occur in response to Harmful UI Patterns do not constitute an intent to interact."***
- We recommend describing potential harmful UI patterns that can occur on each commitment stage of the technology relationship. The Me2B Rules of Engagement described in our Flash Guide 3 is a good resource for understanding when a pattern might be violating the promises of the technology offering.
- In **§ 999.315. Requests to Opt-Out. (h) 1-5.** Opt Out is **not a respectful solution**. We recommend that a respectful default state is one in which no data is collected unless

and until specifically allowed by the user. In part (h), number (2) of this subsection, the consumer choice should be whether to "Opt In" not to whether to Opt Out. Part (h) number (3) would be unnecessary if "Opt Out" were the default. Part (h) number (5) "Do Not Sell My Personal Information" should also be the default for all California residents. Further, California residents should not need to self-identify, because such self-identification may require sharing PII. If this means that the company should make "Opt Out" a default for everyone, then so be it.

- In **§ 999.308. Privacy Policy,** Part (a), number 2(a). Where it states "the privacy policy shall be designed and presented in a way that is *easy to read* and *understandable* to consumers. The policy shall: (a) Use plain, straightforward language and avoid technical or legal jargon.[1] I'd go further to describe tests for readability and understandability, as defined by W3C WCAG 2.1 and described in the Me2B Safe Specification, and also state that a reason to avoid technical and legal jargon is that it can be used as cover for Harmful UI Patterns.

Strategic Overview

The CPRA expressly states that regulations should be adopted to further the purpose of the law including but not limited to adopting regulations that "*does not make use of any dark patterns*."[2] The California Privacy Protection Agency is looking for guidance on Dark Patterns since they have the authority to expand on the current CPRA rules & promulgate new rules to address any issues related to Dark Patterns.

General Ideas for Potential Talking Points

- Do you have any comments on their current CPRA Rule Language? Should they add/expand on something in their rule language?
    - Add a line about dark/deceptive patterns to the definition of "Intentionally interacts" as noted below. DONE
    - Do they only actually bring up Dark Patterns in the consent definition?
    - Perhaps a suggestion to use "Harmful UI Pattern" or "Deceptive UI Pattern" rather than "dark pattern" to avoid the harmful pattern of equating black/white color with good/bad in legislation, but that horse might already be out of the barn at this point. DONE
        - Or not, looks like Harry Brignull recently changed his darkpatterns.org site to https://deceptive.design and is using the phrase "deceptive patterns".
        - The Web Foundation's Tech Policy Design Lab also uses "deceptive patterns" instead of "dark patterns" DONE
            - "A **note on language:** This Tech Policy Design Lab project was originally called "Dark Patterns - Moving Towards Trusted Design'. Though 'Dark Patterns' has been the

[1] California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.308(2)
[2] California Privacy Rights Act, CAL. CIV. CODE §1798.185(a)(20)(C)(iii)

prevailing term to describe the problem for several years, this language reinforces the exclusionary framing that "dark" is "bad" and "light" is "good". That's why, after engaging with our community, we have changed the project name to 'Deceptive Design: Moving Towards Trusted Design Patterns'." DONE

    - We can also address the problem of knowing who is a California resident without ingesting PPI about a user. In our audits we've seen Do Not Sell requests and data deletion forms that require the user to attest that they are a California resident by filling out a long form full of personal information. (May be off topic for dark patterns, but does feel a bit intrusive and potentially unnecessary, and we don't know what they do with this newly collected data or whether it is deleted along with the profile data or retained to satisfy some legal requirement to prove they deleted it.) LISA?

- What issues would you like to see them address in their new regulations? How should they approach those issues?
    - Not requiring Opt Out. Requiring Opt Out is a dark pattern. DONE

    From our Nov 7, 2021 letter to CPPA:

    2. Automated Decisionmaking
    . The scope of consumers' opt-out rights with regard to automated decision-making, and what processes consumers and businesses should follow to facilitate opt outs.

    We object to the mechanism of "opt-out" as it does not promote the safety and wellbeing of people (and isn't harmonized with global norms). Instead, we support the practice of easy to use, opt-in methods.

    Specifically, we advocate for:

    - Safe and respectful default settings, proportional to the nature of the automated decisions,

    - The elimination of coercive harmful patterns used to manipulate people into vendor-preferred behaviors, and

    - [In the absence of respectful defaults] People must be able to reasonably disable "smart" capabilities. For example, Twitter allows the user to change the feed to a chronological-based view, effectively disabling the default "top tweets" feed setting. (Disturbingly, however, the Twitter UX refers to the "top tweets" setting as "Home," which is a dark pattern and disrespectful default). DONE

    And

5. Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit

the Use and Disclosure of their Sensitive Personal Information. What businesses should do to provide consumers who have previously expressed an opt-out preference via an opt-out preference signal with the opportunity to consent to the sale or sharing of their personal information or the use and disclosure of their sensitive personal information.

Our primary guidance here is that businesses must not employ manipulative practices in the UX (I.e. dark patterns) in order to get people to opt back into data selling. We have published clear recommendations around how a website or app should behave with respect to online transactions in our "Attributes of Safe and Respectful Me2B Commitments".

Additionally, it's clear that people need software tools to manage their online relationships at scale. A trusted browser can be such an agent to manage permissions and preferences outside of the Me2B Marriage state.

- Are they still using a toggle switch graphic in their logo? Any UI element that does not look like what it is (a static graphic that looks like a switch) can be interpreted to be a harmful UI pattern) DONE, needs review
- Avoid the problem GDPR created where the solution introduces more harmful patterns than the original problem. [Not discussing GDPR]

- What research and/or research findings would you like to share with the Agency that can help them get in the right mindset when establishing these new regulations?
  - Purdue University, UXP2 Lab https://www.nsf.gov/awardsearch/showAward?AWD_ID=1657310
  - **Gray, C. M.,** Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021, May). Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. In *CHI'21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. New York, NY: ACM Press. https://doi.org/10.1145/3411764.3445779 [preprint at Arxiv]
  - **Gray, C. M., Chen, J., Chivukula, S. S., & Qu, L.** (2021). End User Accounts of Dark Patterns as Felt Manipulation. *Proceedings of the ACM: Human-Computer Interaction, 5*(CSCW2), Article 372, 25 pages. https://doi.org/10.1145/3479516
  - Here's the article I wrote for *Boxes and Arrows*, summarizing my talk on Dark Patterns last year: https://boxesandarrows.com/designing-respectful-tech-what-is-your-relationship-with-technology/ (The video from IAC21 is in our library. It may go behind a paywall at some point but I have the original recording.)
- Exactly what UX Designs will constitute a dark pattern remains unclear.

- We can cite our rules of engagement here. Anything that reduces the agency of the user whether directly or through emotional manipulation. DONE
- We can also point to Harry Brignull and Purdue UXP2's work documenting examples of dark patterns as very clear harmful UI pattern libraries. DONE

Current CPRA Rule Language

"Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, *as further defined by regulation.*[3]

- Is there a legal definition of "substantial effect"? It sounds like it's in the definition: designers are responsible for the effect.

"Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. **Likewise, agreement obtained through use of dark patterns does not constitute consent.**[4]

Below is CPRA Rule Language that does not expressly mention "Dark Patterns" but that might be of interest to you.

"Intentionally interacts" means when the consumer intends to interact with a person, or disclose personal information to a person, via one or more deliberate interactions, including visiting the person's website or purchasing a good or service from the person. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a person.[5]

- Opening a web site can't be considered an intention to interact. People accidentally open websites all the time whether by dark patterns or mistake: misspelling, clicking the wrong link, phishing, reloading a browser tab they thought was closed, swiping a piece of screen "dust" that's actually a UI, etc. Perhaps this clause should include a similar statement to the "consent" definition: ***Likewise, user behaviors that occur through use of dark patterns do not constitute an intent to interact.*** DONE

[3] California Privacy Rights Act, CAL. CIV. CODE §1798.140(L)
[4] California Privacy Rights Act, CAL. CIV. CODE §1798.140(H)
[5] California Privacy Rights Act, CAL. CIV. CODE §1798.140(S)

- A Dark Pattern is a UI pattern. This sounds more like an algorithmic pattern. Something beneath the UI that interprets an interaction to indicate consent. So if the UI interaction (hover, click, tap, focus, scroll) triggers the algorithm it would count. Of course intention is difficult to define. I might scroll past an image and then scroll back up to re-read the paragraph before it. Will the algorithm accept that behavior as intentional just because the advertising image is visible for a minimum amount of time to trigger it? DONE
    - Also the language is a little weird. The examples sound like indications they don't intend to interact, not that they do. Or are they just stating the obvious?

A business's methods for submitting request to opt-out *shall be easy* for consumers to execute and *shall require minimal steps* to allow the consumer to opt-out. A business shall not use a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out. Illustrative examples follow:[6]

> (2) A business shall not use confusing language, such as double-negatives (e.g., "Don't Not Sell My Personal Information"), when providing consumers the choice to opt-out.
>
> (3) Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request.
>
> (5) Upon clicking the "Do Not Sell My Personal Information" link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out.

- **§ 999.315. Requests to Opt-Out. (h) 1-5.** At first these remedies all sound very reasonable, except that requiring people to Opt Out is **not reasonable** in the first place. We recommend that a respectful default state is one in which no data is collected unless and until specifically allowed by the user. In (2) the consumer choice should be whether to "Opt In" not to opt out. The "Opt In" state should not be the default. Part (3) would be unnecessary if "Opt Out" were the default. Part (5) "Do Not Sell My Personal Information" should also the default for all California residents. Further, California residents should not need to self-identify. If this means that the company should make "Opt Out" a default for everyone, then so be it.

The privacy policy shall be designed and presented in a way that is *easy to read* and *understandable* to consumers. The policy shall: (a) Use plain, straightforward language and avoid technical or legal jargon.[7]

- This is reasonable. I'd go further to describe tests for readability and understandability, as defined by W3C WCAG 2.1 which has additional guidance for addressing people with cognitive disabilities. (Does CCPA mention W3C WCAG 2.1? I think it does, but I don't recall if it is specific to that version.)

---

[6] California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.315(h)
[7] California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.308(2)

- Is there a legal construct for "avoid"? What does "avoid technical or legal jargon" actually mean in a legal context?

Additional Notes/Resources

- In October 2021, the FTC released an enforcement policy statement that they would Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions.[8]
    - "sign-ups must be clear, consensual, and easy to cancel"
    - Bye, bye, "Roach Motel." That's just one of many dark patterns.
- Here are the slides for Jennifer King's presentation on Dark Patterns to the California Privacy Protection Agency in March 2022. If your interested in watching or listening to that presentation (click here).
    - King mentions that enforcement should be focused on the outcomes of the design and not the intent of the UX designer. Do you agree?
        - It's in the definition of "dark patterns" that the company at least is responsible for any UI design that has a "substantial effect" on the user's autonomy.
        - In "Ruined By Design," Mike Monteiro states that designers are responsible for the outcome of their designs. https://www.ruinedby.design/ (Mule Books, 2019)
            - "The combustion engine which is destroying our planet's atmosphere and rapidly making it inhospitable is working exactly as we designed it. Guns, which lead to so much death, work exactly as they're designed to work.... Twitter's toxicity and lack of civil discourse is working exactly as it's designed to work."
            - "The world is working exactly as designed. And it's not working very well. Which means we need to do a better job of designing it. Design is a craft with an amazing amount of power. The power to choose. The power to influence. As designers, we need to see ourselves as gatekeepers of what we are bringing into the world, and what we choose not to bring into the world."

[8] FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions, Federal Trade Commission, https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions, Oct. 28, 2021.

Me2BA Rules of Engagement (referenced above)
https://me2ba.org/flash-guide-3-the-me2b-rules-of-engagement-our-ethical-foundation/

- **Freedom |** We agree not to coerce or manipulate each other.
    - This covers many of the items in the Brignull and Purdue deceptive design taxonomies. If the sole purpose of the pattern is to delay or redirect the user from an intended action, then it violates CPRA.
- **Respect of Boundaries |** We agree to respect each other's personal boundaries.
    -
- **Respectful Defaults |** In the absence of stated preferences, we default to the most conservative behavior.
    - In this case, Opt Out should be a default, not a choice that requires an action by the consumer. Requiring Opt Out action is a harmful pattern and violates CPRA.
- **Fairness & Non-exploitation |** We agree to treat each other fairly and not exploit things that are shared.
    - If there is a legitimate purpose for the use of someone's data, then all uses should conform to that purpose, even those uses by a third-party data collector or controller. If a pattern attempts to exploit, share or use the information in a way that is not covered by the legitimate purpose, and if a third-party data collector or controller uses it in a way that is not covered by legitimate, then the pattern violates CPRA.
- **Good Communication |** We agree to be forthright, honest and clear in our communication.
    - The language used in any interaction should be clear, succinct and easy to understand by humans and assistive devices. If it is not, then the pattern violates CPRA.
- **Promise-Keeping |** We keep our promises.
    - If a UI pattern coerces someone into behaviors including data sharing or accepting conditions that the technology claimed it wouldn't require, then the pattern violates CPRA.
- **Non-Harming |** We agree not to willfully harm one another.
    - The UX Outcome is important in determining whether there is harm. While we state that technologies should not willfully harm its users, there is a kind of willful neglect in adopting UI patterns just because they are easy, or because they embedded in the system we use to design a product.
- **Respectful Dispute Resolution |** We agree to respectful, collaborative and fair dispute resolution methods.

CPPA Comments on Audits

Thank you! I'm Lisa LeVasseur, and the founder and executive director of the Me2B Alliance, and I want to take this moment to mention that we've changed our name to Internet Safety Labs. We are a non-profit product safety testing organization for connected technology. We have just released our first open safety specification spec for mobile apps and websites, which was several years in the making. In addition, we have been conducting substantial research and audits particularly in the K12 edtech mobile apps space for the past couple years.

Through the guidance and support of seasoned data supply experts like Zach Edwards, we've honed our product auditing skills and methodologies over the past few years. In particular, our audits look at safety from two key lenses: (1) data flow in and out of the app or website, and (2) harmful patterns (mainly of manipulation) in the user experience. It is based on this experience that we offer the following recommendations for guidance in establishing CPPA Audit practices and policies. We provided more in-depth feedback in our written feedback from last year.

Our comments today focus on three key areas: (1) Scope of Annual Audits (2) Scale considerations, and (3) Ethical Considerations.

1. Scope of discretionary annual audits described in Section 15 A:

a. We note that this is currently described as a "cybersecurity audit". This language is inadequate, as "cybersecurity" doesn't address the full scope of what needs to be audited. We recommend that the annual audit include auditing of privacy- and safety-protecting practices and behaviors. I.e. beyond what is currently understood as "cybersecurity". Note that this covers org and technology behavior.
    i. Further, the scope of testing should have as it's core an independent audit of the *behavior* of the technology.
b. This annual auditing should measure the actual behavior of the technology as its primary focus—not just what the org says it's doing.
c. We recommend independent auditing of three key behaviors of the technology:
    i. Data Supply behavior
    ii. Harmful Patterns behavior in the UX
    iii. Automated Decision-making behavior

2. Scale Considerations:
    a. Auditing is too large a job for a single entity. It will need a network of authorized independent, auditing entities.
        i. As noted in our written comments, we suggest focusing on one industry at a time, developing domain expertise on a particular industry, as tech behaviors need to be understood in the context of industry norms.
    b. Frequency of audits: behavior of technology can be changed with every software update. An annual-only audit of tech behavior will be inadequate.

c. Explore & invest in the development of automated tools for detecting data flow in apps and websites. Auditing of technology is a significant, labor-intensive activity.
d. Develop a mandatory software bill of materials ("ingredients label") for mobile apps and websites to facilitate auditing.

3. Ethical Considerations:
    a. Preserving anonymity:
        i. Annual discretionary Audits: from our experience, we are able to audit technology behaviors (esp data supply behavior and harmful pattern behavior) via black-box testing—meaning, we don't need access to any internal, private information.
        ii. We believe privacy considerations apply more to Ad Hoc violation claims, and we provided guidance in our written response in December.
    b. We STRONGLY recommend that authorized auditing entities be completely divorced from industry—no financial support, and no affiliation with any industry interest organizations. Care must be taken in ethically aligning incentives and business models to ensure the safety and privacy of people first and foremost. Historically, industry organizations have not reliably audited for privacy and safety of their products.
        i. Authorized auditing entities must be independent organizations.
        ii. We're advocating for inclusivity, transparency, and accountability:
            1. Transparency in qualifying criteria, selection, and ongoing performance of authorized

auditors. i.e. publication of all of these things on an ongoing basis.

a. Note that this entails annual auditor assessments/evaluations.

We hope that this input is helpful, in addition to our written comments, and look forward to hearing your thoughts and synthesis on all the comments. Thank you for this opportunity.

References from law:

(15) Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to:

(A) Perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent. The factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities.

(B) Submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that

processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public. Nothing in this section shall require a business to divulge trade secrets.

(18) Issuing regulations to define the scope and process for the exercise of the agency's audit authority, to establish criteria for selection of persons to audit, and to protect consumers' personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena.