Internet Safety Labs CPPA Pre-Rulemaking Comments May 2022

Stakeholder Comments on Auditing

Lisa LeVasseur, Founder and Executive Director, Internet Safety Labs

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 (especially 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.

<u>References from the law</u>

§1798.185 (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.

§1798.185 (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.

Stakeholder Comments on US and Dark Patterns

Noreen Whysel, Director of Validation Research, Internet Safety Labs

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, wellknown 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 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.

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.
- Referencing §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 Pll. If this means that the company should make "Opt Out" a default for everyone, then so be it.
- Referencing §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. 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.