



LEGAL UPDATES

Beware of Dark Patterns – What to Watch Out For

Although businesses that are CCPA compliant can use their current framework as a starting point for CPRA, addressing dark patterns is a new statutory requirement introduced by CPRA that businesses should begin preparing for now.

07/20/2022 | 3 minute read

On May 27, the California Privacy Protection Agency released its draft regulations for the California Privacy Rights Act (CPRA). The agency was required to adopt final regulations by July 1, 2022 – nearly six months before CPRA is set to go into effect on January 1, 2023. However, the final regulations have been stalled and they will likely not be issued until later this Fall.

Albeit the regulations are still in draft form and not final, businesses should use such draft regulations as a roadmap for CPRA compliance. Although businesses that are CCPA compliant can use their current framework as a starting point for CPRA, addressing dark patterns is a new statutory requirement introduced by CPRA that businesses should begin preparing for now.

The text of CPRA defines a “dark pattern as 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)^[1]. Importantly, an agreement by a user that is obtained through use of dark patterns does not constitute consent. Companies that purportedly obtained user consent to their terms of use or other agreements that used dark patterns cannot rely on this as valid consent.

The term, originally coined in 2010 by Harry Brignull, has caught traction by legislators, regulators, and attorneys general. Last year, the FTC hosted a workshop explaining dark patterns and subsequently issued a policy statement, announcing that it would prioritize enforcement against dark patterns, specifically those relating to recurring subscription fees^[2]. So, CPRA is not alone in prioritizing the enforcement against dark patterns^[3].

Section 7004 of the draft regulations makes explicit, under a “consent” heading, that dark patterns used to obtain consent would vitiate consent. In addition, Section 7004 covers dark patterns affecting methods for submitting CCPA requests. Particularly, the regulations are potentially broader than the terms in CPRA because the dark pattern rules would also apply to other user interface architectures, including the form a website uses to collect user right requests to correct or delete data.

Related People

Chiara Portner, CIPP/US

Partner

Redwood Shores

650.804.7672

chiara.portner@lathropgpm.com

Related Services

[Data Privacy &](#)

[Cybersecurity Compliance](#)

Related Sectors

[Retail & E-Commerce](#)



The draft regulations announced five guiding principles to avoid invalidating consent through dark patterns. The user interface architecture must:

1. ***Be easy to understand.*** No legalese. Language must be easy to read and understand.
2. ***Provide symmetry in choice.*** Path for a consumer to exercise a more privacy-protective option must be no longer than the path to exercise a less privacy-protective option. For example, designs where the “yes” button is more prominent or a different color than the “no” button would vitiate consent.
3. ***Avoid language or interactive elements that are confusing to the consumer.*** Toggles and buttons must clearly indicate a consumer’s choice. For example, use of double negatives or unexplained toggles would vitiate consent.
4. ***Avoid manipulative language or choice architecture.*** Shaming or using guilt to manipulate a consumer into making a particular choice or bundling consent to subvert consumer’s choice would vitiate consent. For example, “I like paying full price” warnings or requiring a consumer to click through reasons against their choice would vitiate consent.
5. ***Be easy to execute.*** Unnecessary burden or friction for a consumer seeking to exercise privacy rights. For example, “Do Not Sell” links that require searching or scrolling to find the opt-out mechanism would vitiate consent.

These regulations are broad and flexible, which may sweep in a host of everyday business practices not closely monitored by legal and compliance departments. Consumer conscious businesses should do their best to ensure their current and future practices do not put them at risk of dark pattern enforcement actions.

Existing websites, new websites, and product campaigns should be reviewed to ensure their design interfaces do not deceive or manipulate consumers – this applies to online and offline business practices. Of note and as a long standing overarching privacy rule, companies should be transparent with consumers about how their personal data is collected, used, and shared. Companies should evaluate designs or tactics that could be considered manipulating consumer choice, which includes privacy choices and commercial choices, like auto-renewals.

Failure to do so may result in invalidating consumer consent, risking dark pattern enforcement actions, and undermining a company’s reputation with consumers. As dark pattern regulation continue to proliferate, so does the risk. Lathrop GPM can help your business mitigate this risk.

For more information, please contact [Chiara Portner](#).

[1] [Cal. Civ. Code 1798.140.\(l\)](#)

[2] Bringing Dark Patterns to Light: An FTC Workshop, Federal Trade Commission (April 29, 2021), available at <https://www.ftc.gov/news-events/events-calendar/bringing-dark-patterns-light-ftc-workshop>; FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions (Oct. 28, 2021), available at <https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions>.

[3] The FTC, using its authority under both the “unfair” and “deceptive” prongs of Section 5, will be bringing actions against dark patterns practices.