Published on *The National Law Review* https://natlawreview.com

Beware Dark Patterns – What are They and What Should Your Business Do About Them?

Article By:

Brian H. Lam

While the term “dark patterns” is not new, it has recently been getting a more attention, not least because the newly passed California Privacy Rights Act (“CPRA”) will regulate dark patterns. In this article, we will focus on what dark patterns are, how your business should be thinking about them, and how CPRA is approaching this issue.

What are Dark Patterns?

The term dark patterns stems back to comments made by user interface expert Harry Brignull on or around 2010, which he described as mechanisms that could be employed within software to discourage users from taking actions that the entity employing the mechanism did not want the user to take, such as unsubscribing from a mailing list, or completing actions that they would not otherwise take, such as sharing personal information.

Effectively, dark patterns can be thought of generically as using insidious methods within the user interface portion of an offering to influence user behavior in ways that the user would not expect or desire. Of course, there is not always malicious intent, and exactly what does or does not constitute a dark pattern is up for debate.

What does the CPRA say about Dark Patterns?

The CPRA approach to dark patterns gives regulated entities some less than clear guidance.

- Dark patterns as defined 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.”

- The CPRA has added a newly defined “consent” such that “agreement obtained through the use of dark patterns does not constitute consent.”

- Implementing regulations involving the sale or sharing of personal information will be required to ensure that a business obtaining consumer consent for sale or sharing of personal information “does not make use of any dark patterns.”

Thus, while it is clear that certain user interface designs could render any such “consent” invalid in the future, exactly what will constitute dark patterns remains somewhat opaque.

Given the uncertainty, what steps should regulated entities take?

Here are a few steps regulated entities can take to reduce their dark pattern risk:

- Be cognizant of the issue generally. Consider working with your user interface design colleagues to inform them of the contours of the issue, and ask them if they think any of their design decisions could be considered dark patterns. Pay particular attention to information collection elements, or areas where the system is attempting to obtain effective user consent.

- The space is evolving. Consider attending a workshop such as this one, being held by the FTC on dark patterns.

- As part of your own internal privacy by design process, institute a review process for your entity’s information collection surfaces, such that important user interface areas are reviewed by neutral members of your organization or a third party.

National Law Review, Volume XI, Number 92

Source URL:https://natlawreview.com/article/beware-dark-patterns-what-are-they-and-what-should-your-business-do-about-them