

California Announces Dark Patterns as an Enforcement Priority

With a growing number of states having passed comprehensive consumer data privacy laws (19 in total, with seven passed this year alone), state enforcement actions related to data privacy are growing increasingly common. Earlier this year, the California Privacy Protection Agency (CPPA), which is tasked with administering and enforcing the California Consumer Privacy Act (CCPA), outlined its updated enforcement priorities. In addition to prior areas of focus, the agency would also prioritize combatting dark patterns.

What are Dark Patterns?

Dark patterns (also referred to as deceptive design patterns) are user interfaces that have been designed in a manner that guides users into taking certain actions or making certain decisions. Some definitions of dark patterns require intention on the part of the developer, while others allow for the inadvertent creation of dark patterns. In the context of data privacy, the term is most often used to refer to user interfaces that steer individuals away from settings that afford higher levels of privacy protection, such as rejecting cookies.

Pinning down exactly what qualifies as a dark pattern can be difficult. While it is true that, in certain instances, dark patterns are intentionally implemented, this is not always the case. Often, dark patterns emerge unintentionally. In the context of consumer privacy, this can occur when a new law, such as the CCPA, requires that a company afford consumers new privacy-friendly choices. If a company tacks this choice onto an existing user interface, and it is not readily apparent to a user that they have that choice or exercising it is difficult, the company may have inadvertently created a dark pattern.

The CCPA has its own definition of a dark pattern: “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice.” The law also requires the CPPA to provide further specificity, which it did through regulations finalized in March 2023 (the Regulations). Deputy Director of Enforcement Michael Macko has expressed that intent is not required under the CCPA, stating, “[d]ark patterns *aren’t about intent*, they’re about effect.”¹

CCPA Enforcement Advisory

Even with the additional context provided in the Regulations, identifying a dark pattern can be difficult. To help provide additional clarity, on September 4, the CPPA issued an “Enforcement Advisory” entitled “Avoiding Dark Patterns: Clear and Understandable Language, Symmetry in Choice” (the Advisory).

The Advisory pulls together the various provisions related to evaluating dark patterns under the CCPA. These serve to remind companies of the concepts they should keep in mind when developing user interfaces, including that they are easy to understand, use plain, straightforward language and avoid technical or legal jargon, and employ symmetry in choice. The Advisory also includes several illustrative examples of symmetry in choice (or lack thereof) provided by the Regulations. For instance, an opt-in process that presents “yes” and “ask me later” as options



Christopher Dodson

Member

cdodson@cozen.com
Phone: (215) 665-2174
Fax: (215) 372-2408



Daniel Kilburn

Associate

DKilburn@cozen.com
Phone: (215) 665-4726
Fax: (215) 665-2013

Related Practice Areas

- Business
- Technology, Privacy & Data Security

does not represent symmetry of choice, while one that uses “yes” and “no” does.

Next, the Advisory lays out a hypothetical scenario in which a business is considering various user interface options. The scenario offers visual examples that will be immediately familiar to anyone who has spent enough time online. While the Advisory encourages the reader to consider whether the examples may represent dark patterns, it does not offer an opinion on the matter.

Finally, the Advisory offers five questions a company can ask itself when considering whether a particular user interface represents a dark pattern:

- Is the language used to communicate with consumers *easy to read and understandable*?
- Is the language *straightforward*, and does it *avoid technical or legal jargon*?
- Is the consumer’s path to saying “no” *longer* than the path to saying “yes”?
- Does the user interface make it *more difficult* to say “no” rather than “yes” to the requested use of personal information?
- Is it more *time-consuming* for the consumer to make the more privacy-protective choice? ²

Overall, the Advisory reminds businesses to carefully evaluate how they offer privacy choices to consumers in each instance to ensure that they do not represent a dark pattern. It also serves as a useful reference guide for the relevant provisions in the CCPA and Regulations and may help illuminate some of the CPPA’s thinking on the subject.

As legal requirements related to consumer privacy continue to grow, it can be easy to unintentionally design or implement a user interface that includes dark patterns. Any entity subject to the CCPA should carefully evaluate the interfaces and paths they use to present consumers with privacy-related choices to ensure they do not represent a dark pattern.

¹ emphasis added

² emphasis in original
