

# California Privacy Protection Agency Issues Dark Pattern Enforcement Advisory

September 05, 2024

On September 4, the California Privacy Protection Agency [issued an enforcement advisory](#) regarding “choice architectures that have the substantial effect of subverting or impairing a consumer’s autonomy, decision-making, or choice” which are, in other words, considered “dark patterns” pursuant to the California Consumer Privacy Act (CCPA) and its implementing regulations. This advisory indicates that the CPPA is closely scrutinizing consents for dark patterns and will consider such consents invalid. If the agency determines consumer consent is invalid due to a dark pattern, it could lead to allegations that all processing activities on which that consent is based are unlawful and subject to civil penalties of up to \$2,500 per violation, and up to \$7,500 for willful violations. In its advisory, the agency reminds businesses and service providers to “carefully review and assess their user interfaces,” including consent management platforms, to ensure that consumers are offered “symmetrical” choices and that such choices are conveyed using plain language. A symmetrical choice refers to the ability of a consumer to exercise a more “privacy-protective” choice as easily as they may exercise a less privacy-protective choice. Essentially, “dark patterns are about effect, not intent.” Examples of equal vs. problematic choices are included in the

Not symmetrical or unequal choice	Symmetrical or equal choice
<p>When the business’s process for opting out of the sale/sharing of their personal information takes more steps than the process to opt back in.</p> <p>See 11 CCR § 7004(a)(2)(A).</p> <p>A process to opt-in to the sale of personal information that only gives the choice of “yes” and “ask me later.”</p> <p>See 11 CCR § 7004(a)(2)(B).</p>	<p>A website banner seeking the consumer’s consent to use a consumer’s personal information that offers the choices “Accept All” and “Decline All.”</p> <p>See 11 CCR § 7004(a)(2)(C).</p> <p>A process to opt-in to the sale of personal information that gives the choice of “yes” and “no.”</p> <p>See 11 CCR § 7004(a)(2)(B).</p>

advisory:

The advisory

encourages businesses assessing their user interfaces or consent flows to ask:

- Is the language easy to read, in plain language, and free of legal jargon?
- Is the consumer's path to the less privacy-protective choice longer or more difficult to reach than the more privacy protective choice?
- Is it more time-consuming for a consumer to make a more privacy-protective choice?

## Authored By



Elliott Siebers



Patricia M. Carreiro

## Related Practices

[Cybersecurity and Privacy  
Technology](#)

## Related Industries

[Technology](#)

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.

