

DO DARK PATTERNS LURK ON YOUR WEBSITE? 4 STEPS BUSINESSES SHOULD TAKE AS REGULATORS FOCUS ON HOW PRIVACY RIGHTS ARE PRESENTED ON WEBSITES

Insights
Sep 9, 2024

Businesses with a website beware: California regulators just warned that the law prohibits your website from making website users jump through hoops or otherwise confusing them as they try to exercise their privacy rights, regardless of whether you intend to have that effect. If your website can be accessed by California residents, regardless of where your business is located, this news may impact your business. The California Privacy Protection Agency published its second Enforcement Advisory warning about the use of “dark patterns” – those interfaces that impair a website user’s ability to make a choice regarding the collection, use, or disclosure of their personal information – on September 4. It reflects the Agency’s focus on how privacy choices, particularly consent to use of cookies and other similar technologies on websites, are presented to consumers in compliance with the California Consumer Privacy Act (CCPA). What are the four steps you should take to ensure you comply with this latest warning?

2 Key Takeaways

The two key takeaways from last week’s release are:

- You can’t make consumers jump through **unnecessary hoops** to exercise their privacy rights; and
- Your **intent is irrelevant** where the effect is consumer confusion or if it makes it less likely that consumers would exercise their rights or make an informed choice.

Related People



Kate Dedenbach, CIPP/US
Of Counsel

248.901.0301



Usama Kahf, CIPP/US
Partner

949.798.2118

Dark Patterns Under the Microscope

The Enforcement Advisory restates the CCPA definition of dark patterns and provides the main requirements for you to avoid them. To avoid a dark pattern, a website operator should ensure that your website presents privacy choices (such as cookie preferences) to users in an easy-to-understand manner, in plain language.

The Agency also warned against your website providing a lack of symmetry – such as only giving users the choice to accept cookies without a reject option, or giving the choice to accept along with an “X” in the corner (which some consumers might think is the reject option when it just simply closes the cookie banner). A website that requires more steps to make a privacy protective choice than a less privacy protective choices may lack symmetry and may be considered a dark pattern.

Intent is Irrelevant

The Advisory also makes clear that the Agency will not consider the intent of the website owners or operators when evaluating the website for dark patterns. Its focus, instead, will be on the impact to the consumer. Regardless of whether the intent to fully inform the consumer was present, you may be at risk of an enforcement action if the ultimate result does not include a readable, easy-to-understand, accessible, and easy-to-use informed choice presented to the website user.

4 Steps to Ensure Your Website Privacy Choices Avoid Dark Patterns

Ask yourself these four questions about your business website to determine whether you could face dark pattern problems:

1. Does Your Cookie Information and Privacy Notice Use Plain Language?

If your notice to consumers uses difficult-to-understand legal terms and confusing language, or offers options that are difficult to understand, you may have a dark pattern. You should clearly explain what data is being collected and how it will be used or disclosed – but do it in a way that a non-technical person would understand. Avoid long sentences with many subparts.

Service Focus

[Consumer Privacy Team](#)

[Digital Wiretapping Litigation](#)

[Privacy and Cyber](#)

Related Offices

[Irvine](#)

[Los Angeles](#)

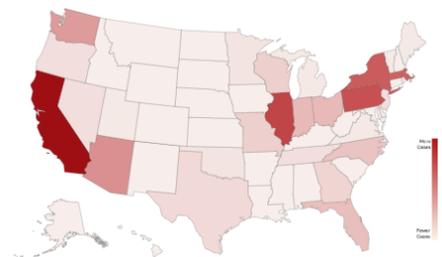
[Sacramento](#)

[San Diego](#)

[San Francisco](#)

[Woodland Hills](#)

Wiretapping Litigation Map



2. Does the Cookie Banner Provide a Link to the Privacy Policy or Cookie Preference Center?

Here are some signs that you may have a dark pattern on your website:

- If your cookie banner or pop-up doesn't offer a one-click link to your Privacy Policy, Cookie Policy, or Cookie Preference Center where more information can be found to inform privacy choices.
- If website users need to click through multiple screens or go back to the main page to find the Privacy Policy and Cookie information.
- If the link to your Privacy Policy is hiding behind the cookie banner such that a user must select one of the options presented for it to go away and for them to be able to access the Privacy Policy and learn about the choice they were just compelled to make.

3. Does the Cookie Banner Offer Only an "Accept Cookies" Option?

If your website cookie banner options include "Accept All" or "Accept Cookies," but doesn't similarly offer a "Decline" or "Reject Cookies" option, this could be considered a lack of symmetry and therefore a dark pattern that increases the risk of an enforcement action. Similarly, if declining any cookies requires users to visit more screens than accepting cookies, this may also indicate a lack of symmetry and may be considered a dark pattern.

4. Does Your Cookie Banner Use a Font That is Too Small?

If the cookie banner and other privacy preferences are not visible enough and are considered too small or difficult to read in relation to the other website fonts and design elements, this may be considered a dark pattern.

Conclusion

Fisher Phillips will continue to monitor the situation and provide updates as warranted, so make sure you are subscribed to [Fisher Phillips' Insight System](#) to get the most up-to-date information direct to your inbox. For further information, contact your Fisher Phillips attorney, the authors of this Insight, or an attorney on the firm's [Consumer](#)

[Privacy Team](#) or [Privacy and Cyber Team](#). You can also visit our firm's [CCPA Resource Center](#) at any time.