AN A.S. PRATT PUBLICATION
NOVEMBER-DECEMBER 2024
VOL. 10 NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 10 **NUMBER 9** **November-December 2024**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2024–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Do Dark Patterns Lurk on Your Website? 4 Steps Businesses Should Take as Regulators Focus on How Privacy Rights Are Presented on Websites

By Kate Dedenbach and Usama Kahf*

In this article, the authors offer four steps that business should take to ensure they comply with a new enforcement advisory from the California Privacy Protection Agency.

Businesses with a website beware: California regulators have 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 has 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. 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?

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.

* The authors, attorneys with Fisher Phillips, may be contacted at kdedenbach@fisherphillips.com and ukahf@fisherphillips.com, respectively.

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.

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 does not 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

The two key takeaways from the Enforcement Advisory are:

- You cannot 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.