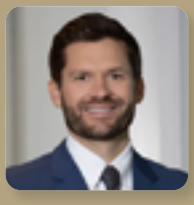
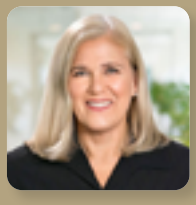
# UNCLOAKING DARK PATTERNS: IDENTIFYING, AVOIDING, AND MINIMIZING LEGAL RISK



**BY KYLE R. DULL**



**& JULIA B. JACOBSON**

Kyle R. Dull is a senior associate in the Data Privacy, Cybersecurity & Digital Assets Practice at Squire Patton Boggs (US) LLP. He previously served as an Assistant Attorney General prosecuting consumer protection and privacy related offenses. Julia B. Jacobson is a partner in the Data Privacy, Cybersecurity & Digital Assets Practice at Squire Patton Boggs (US) LLP.

# TechREG CHRONICLE
# MAY 2023



Visit www.competitionpolicyinternational.com for access to these articles and more!

## UNCLOAKING DARK PATTERNS: IDENTIFYING, AVOIDING, AND MINIMIZING LEGAL RISK

By Kyle R. Dull & Julia B. Jacobson

Regulators have long targeted deceptive and misleading practices designed to manipulate consumers, including more recently "dark patterns." Dark patterns are misleading or otherwise manipulative user experiences intended to influence a consumer's behavior and prevent them from making fully informed choices. Dark patterns are not merely clever marketing gimmicks; rather, they are designed to cause users to unwittingly act against their personal preferences, such as signing up for services they do not want, purchasing products they do not intend to purchase, sharing personal information. In this article, we review common dark patterns and how they are used in today's digital world. We also analyze consumer protection and privacy regulatory developments targeting dark patterns and discuss best practices for digital service operators to help minimize regulatory sanctions, class actions and reputational damage arising from dark pattern practices.

Dark patterns are misleading and manipulative design choices intended to influence a consumer's behavior and prevent them from making fully informed decisions about their data and purchases. Dark patterns go beyond clever marketing gimmicks and instead cause users to unwittingly take action against their personal preferences, such as signing up for services they do not want, purchasing products they do not intend to purchase, or surrendering their personal information.

Dark patterns are highly effective at influencing consumer behavior, particularly with less sophisticated users and when layered together. In a recent enforcement action,[2] dark patterns in gaming apps resulted in unauthorized charges because, where a button to advance to the next level is placed immediately proximate to a "buy" button, which automatically generated charges when accidentally bumped or an app advertised as "free" had hidden charges described as qualifiers in fine print placed far from the term "free." These practices caused unaware players to rack up charges, ranging from a dollar to hundreds of dollars, frequently on their parents' credit cards, from the use of a single app or website. While dark patterns are most commonly used in online settings, they also are found in physical stores, and across industries.

Although the term "dark patterns" was coined over a decade ago by Harry Brignull,[3] recently, the consequences of dark patterns have recently received increased consumer protection and privacy regulatory and legislative attention in the United States, EU, and UK.

# 01
# TYPES OF DARK PATTERNS

Dark patterns can be difficult to spot but some of the most commonly used forms include:

· ***Misdirection***: A business uses distracting language or visuals such that users do not fully understand to what they are agreeing. The user interface's design focuses a user's attention on one thing in order to distract the user's attention from another element.

· ***Bait and Switch***: A business offers a product or service at a low price, but then makes the actual purchase process especially complex. A user thinks that their action will have a specific outcome, but in the end, it does not materialize. For example, a business might require users to create an account or enter credit card information before the final price is presented.

· ***Nudging***: A business uses subtle psychological tricks to influence users' behavior by using contrasting visual prominence to steer users into making a certain selection, such as bright colors or bold fonts to make certain options stand out more than others.

· ***Overloading***: A business sends users numerous requests or offers numerous options in order to deter certain actions or manipulate users to unintentionally share or allow the processing of their personal data.

· ***Skipping***: A user interface is designed to cause users to forget or overlook data protection concerns or options.

· ***Shaming*** or ***Stirring***: A business manipulates user choice with emotional steering, e.g. an option to decline is worded in such a way as to shame the user into compliance.

· ***Hindering***: The user experience includes dead end choices or other tactics that make it difficult or impossible for users to obtain information or take action.

· ***Fickle***: These practices include disguised ads and inconsistent user interfaces that are confusing or unclear.

· ***Left in the Dark***: Interfaces are designed to hide choice from users or include ambiguous wording, such as conflicting information about how personal information is being processed.[4]

2 See *In the Matter of Epic Games, Inc.* (March 14, 2023), available at https://www.ftc.gov/legal-library/browse/cases-proceedings/1923203-epic-games-matter.

3 See https://www.deceptive.design/about-us (last accessed April 30, 2023).

4 European Data Protection Board ("EDPB"), *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognize and avoid them* (March 14, 2022), available at https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf; Federal Trade Commission, *Bringing Dark Patterns to Light* (September 2022), available at https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

# 02
# EXAMPLES OF DARK PATTERNS

Dark patterns are often used in:

· ***Negative Options***: An online provider employing dark patterns may make the process for purchasing a subscription online relatively easy with a short check-out/purchase flow, but establish a complex, multistep flow process, online or offline, for cancelling the subscription which involves forcing customers to consider different offers designed to prevent them from un-subscribing.
· ***Online Advertising***: A business uses deceptive tactics to cause users to click on ads, such as a fake news article or headline.
· ***Dark Patterns in E-commerce***: An e-tailer uses deceptive tactics designed to cause users to buy more products than intended. For example, a business might use a "buy now, pay later" option or presenting a limited time offer that has no actual deadline or that resets at an arbitrary time (e.g. the limited time offer clock resets when the user refreshes the webpage).
· ***Consumer Ratings***: A "neutral" shopping comparison site ranks choices based on compensation not actual experiences with a product or using phony customer endorsements or presenting other people's experience without revealing material information, such as compensating endorsers or not qualifying an endorser's experiences as atypical.

Dark patterns not only harm individual consumes; they also are anticompetitive. Businesses using dark patterns gain an unfair advantage over competitors by, for example, making fair and accurate price and service comparison difficult because information is hidden or deceptively presented. Businesses may also use dark patterns to prevent consumers from switching to competitors (which may offer better prices or services) by making cancellation difficult, e.g. presenting a "Keep Your Benefits" option as a bright orange button, while presenting the "Cancel Subscription" option as a smaller font, pale gray hyperlink.

# 03
# REGULATORY DEVELOPMENTS IN THE U.S.

Regulators in the U.S. have long targeted unfair and deceptive practices designed to manipulate consumers in certain ways. The digital world is no different.

### *A. Dark Patterns and Consumer Protection*

In September 2020, the Federal Commission announced a $10 million settlement against an online subscription service that operated a deceptive subscription program that inadequately disclosed that 12-month memberships and extensions on 30-day free trial memberships at reduced rates would automatically renew and, despite advertising "easy cancellation," made cancellations nearly impossible. While the settlement did refer to these practices as dark patterns, then FTC Commissioner (and current Director of the Consumer Financial Protection Bureau ("CFPB")) Rohit Chopra issued a statement calling the business practices dark patterns.[5] In the statement, Commissioner Chopra noted: "Dark pattern tricks involve an online sleight of hand using visual misdirection, confusing language, hidden alternatives, or fake urgency to steer people toward or away from certain choices." Director Chopra continues to investigate allegations of digital dark patterns while at the helm of the CFPB.[6] Since then, the Federal Trade Commission ("FTC") released a September 2022 Staff Report, *Bringing Dark Patterns to Light* ("FTC Report").[7] The FTC has finalized enforcement actions against businesses using dark patterns.[8]

5 Federal Trade Commission, Statement of Commissioner Rohit Chopra, *Regarding Dark Patterns in the Matter of Age of Learning, Inc. Commission File Number 1723186* (September 2, 2020), available at https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf.

6 See "CFPB Issues Guidance to Root Out Tactics Which Charge People Fees for Subscriptions They Don't Want" (January 19, 2023), available at https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-guidance-to-root-out-tactics-which-charge-people-fees-for-subscriptions-they-dont-want/ (last accessed April 30, 2023).

7 Federal Trade Commission, *Bringing Dark Patterns to Light* (September 2022), available at https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

8 See e.g. Credit Karma, LLC, available at https://www.ftc.gov/legal-library/browse/cases-proceedings/2023138-credit-karma-llc; RagingBull.com, available at https://www.ftc.gov/legal-library/browse/cases-proceedings/2023073-ragingbullcom; and LendingClub Corporation, available at https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3088-lendingclub-corporation.

Consumer protection laws are not the only options for federal and state regulators seeking to prevent dark patterns. For example, the Restore Online Shopper's Confidence Act ("ROSCA"), a 2012 law targeted to online negative option plans, requires (*inter alia*) clear and conspicuous disclosures of material terms prior to requesting and receiving a customer's billing information for a recurring charge.[9] Effective as of July 1, 2022, California's now-updated automatic renewal law requires that a business provide its California consumers an online subscription cancellation option for a subscription purchased online, without extra steps that obstruct terminating the autorenewal plan.[10] Colorado, Illinois, Maryland, and New York also updated their automatic renewal/negative option laws recently to impose more robust notice and cancelation requirements on businesses offering autorenewal plans.

> ***Consumer protection laws are not the only options for federal and state regulators seeking to prevent dark patterns***

In April 2023, the FTC proposed substantial amendments to the existing Negative Option Rule, setting higher standards for autorenewal promotions and sales than exist under current federal or state laws and regulations.[11] If promulgated, the revised Negative Option Rule will apply to many more businesses and scenarios than are currently subject to autorenewal regulation. The proposed Negative Option Rule would cover all forms of so-called "negative option" marketing and sales in all media, including negative options sold in a business-to-business ("B2B") context (e.g. autorenewal terms in business services contracts), for month-to-month auto-renewing terms (e.g. "no contract" cell, Internet, media or entertainment services and even auto-renewing monthly residential and commercial real estate tenancies) and for both the sale of goods and services. Other notable additions to the Negative Option Rule include enhanced disclosure, consent, and cancellation requirements, as well as a powerful misrepresentation prohibition and annual reminders. Whether or not this proposed Negative Option Rule is finalized by the FTC, it clearly shows that regulators are targeting dark patterns in every sphere of the marketplace.

### *B. Dark Patterns and Privacy*

State privacy laws are also targeting dark patterns. The amended California Consumer Privacy Act ("CCPA"), which will be fully enforced July 1, 2023, targets dark patterns used in the process offered to consumers for opting out of the sale and sharing of personal information, among other areas.[12] For example, the consent web page must "allow[] the consumer . . . to revoke the consent as easily as it is affirmatively provided."[13] The link to the consent web page cannot "not degrade the consumer's experience on the web page the consumer intends to visit and has a similar look, feel, and size relative to other links on the same web page."[14] The regulations implementing the CCPA, as amended by the California Privacy Rights Act ("CPRA"), go even further and state, "[a] business's intent in designing the interface is not determinative in whether the user interface is a dark pattern, but a factor to be considered."[15]

These requirements are directly targeting dark patterns used by businesses to influence consumer behavior and prevent a consumer from making a fully informed decision about consenting to the business's sale or sharing of the consumer's personal information. Of importance, consent obtained through dark patterns does not constitute "consent" under the CCPA. Dark patterns also are addressed in the Colorado Privacy Act ("CPA"), which specifically defines "consent" as not including an "agreement obtained through dark patterns"[16] and the Connecticut Data Privacy Act which defines dark pattens similarly to CCPA and CPA but also includes "any practice the Federal Trade Commission refers to as a 'dark pattern.'"[17]

9 Restore Online Shopper's Confidence Act, 15 U.S.C. §§ 8401—8405.

10 California Business and Professions Code §§ 17600—17606.

11 Federal Trade Commission, *Negative Option Rule, A Proposed Rule by the Federal Trade Commission* (April 24, 2023), 88 Federal Register 24716.

12 California Civil Code §§ 1798.100—1798.199.100.

13 Cal. Civ. Code § 1798.135(b)(2)(A).

14 Cal. Civ. Code § 1798.135(b)(2)(B).

15 California Code of Regulations Title 11 § 7004(c).

16 Colorado Revised Statutes §§ 6-1-1301—6-1-1313 (effective July 1, 2023).

17 State of Connecticut, Public Act No. 22-15, § 1(11).

Like California, under the Colorado[18] and Connecticut[19] laws, consent obtained through the use of dark patterns is not valid.

While not specifically targeted to dark patterns, the California Age-Appropriate Design Code Act ("CAADCA") addresses dark patterns affecting interactions with minors.[20] Under the CAADCA, businesses are prohibited from "us[lng] dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature to forego privacy protections, or to take any action that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or well-being."[21] Other states are considering laws similar to CAADCA.[22]

And of course, the mini-FTC Acts enforced by the states establish broad powers for the relevant agencies to regulate unfair or deceptive acts and practices – including dark patterns.

In Europe, dark patterns also may violate various provisions of the General Data Protection Directive ("GDPR"),[23] including the fairness and transparency principle (Art. 5(1)(a)), the accountability principle (Art. 5(2)), data protection by design and default (Art. 25), the requirement to provide transparent privacy notices to data subjects (Art. 12(1), 13 & 14), and the data subject rights under GDPR Art. 15-22. Further, Europe's Digital Services Act, which applies to online-platforms, also decrees that "[r]ecipients of a service should be able to make a free, autonomous and informed decisions or choices when using a service and providers of intermediary services shall not use any means, including via its interface, to distort or impair that decision-making. In particular, recipients of the service should be empowered to make decisions, inter alia regarding the acceptance of and changes to terms and conditions, advertising practices, privacy and other settings, recommender systems when interacting with intermediary services."[24] Thus, no matter the medium, regulators are concerned with dark patterns in consumer interactions and are working to prohibit their use.

*"While not specifically targeted to dark patterns, the California Age-Appropriate Design Code Act ("CAADCA") addresses dark patterns affecting interactions with minors*

Dark patterns are also an issue addressed by self-regulatory agencies in the United States. The Network Advertising Industry ("NAI"), which has previously covered regulatory action on dark patterns,[25] published guidance for its members on the topic and issued opinions.[26] Of note, the NAI addresses "light patterns" which "are practices that make proactive decisions on behalf of users, having their best intentions in mind." These practices should also be reviewed carefully, with the goal that the light pattern only advances the user's ability to make informed choices, and does not make the choice on their behalf. A light pattern may evolve into a dark pattern if the business begins to "make assumptions about what is in consumers' best interests run the risk of promoting certain business models over others."[27]

18 Colorado Revised Statutes § 6-1-1303(5).

19 State of Connecticut, Public Act No. 22-15, § 1(6).

20 Cal. Civ. Code §§ 1798.99.28-1798.99.40.

21 Cal. Civ. Code § 1798.99.31(b)(7).

22 See e.g. Maryland Age-Appropriate Design Code Act, HB0901, § 14-4507(7).

23 Regulation 2016/679.

24 Digital Services Act, 2020/0361(COD), Recital 39a.

25 See https://thenai.org/dark-and-light-patterns-when-is-a-nudge-a-problem/.

26 Network Advertising Industry comments filed with the Federal Trade Commission, *Bringing Dark Patterns to Light: An FTC Workshop* (March 15, 2021), available at https://thenai.org/wp-content/uploads/2021/07/nai_comments_ftc_dark_patterns_15march2021.pdf; see also National Advertising Division Recommends Pier 1 Imports Clearly and Conspicuously Disclose Material Terms of Pier 1 Rewards Membership (February 27, 2023), available at https://bbbprograms.org/media-center/dd/pier-1-rewards (last accessed April 30, 2023).

27 Digital Services Act, Regulation (EU) 2022/2065, Recital 39a.

# 04
# HOW TO PROTECT YOURSELF FROM DARK PATTERNS

To reduce the risk of regulatory sanctions, the potential for consumer class actions and reputational damage, online platforms and publishers should be mindful of the increasing focus on dark patterns by U.S. and European regulatory authorities. Best practices include:

· Evaluate current practices to ensure that marketing and website interface design teams are aware of the regulatory risks and requirements.
· Make use of interdisciplinary teams when designing a user experience, including designers, privacy professionals, and decision-makers.
· Consider the audience in designing the user interface. Design for adults, teens, and children may differ.
· Design consent processes to ensure that consent is informed, specific, affirmative, and voluntary.
· Ensure that material terms and conditions are clear, conspicuous, and relevant. The language should be direct, clear and not used to pressure or manipulate consumers into making preferred (by the business) choices.
· Provide accurate and complete information from the start and maintain the information as accurate and complete through the consumer's experience so that consumers are not misinformed or misled.
· Use fair and transparent disclosures presented at or before the consumer action is required, and highlight unusual or unexpected practices.
· View the disclosures from the audience's perspective.
· Check that privacy policies and website terms accurately describe current data practices in a manner that is understandable to the typical consumer.
· Implement Privacy by Design principles and proactively integrate privacy into the design and architecture of systems and business practices. In particular, practice data minimization and collect only the information that you need and focus on transparency.
· Opt-in and opt-out flows should clearly disclose what consumers are opting in and out of, require a similar number of steps (i.e. not make it harder to opt out than to sign up), and be easily accessible to consumers.
· Review consumer concerns regarding the user flow and remedy any identified potential issues as soon as possible.

As a consumer, you can protect yourself from dark patterns:

· Be aware of the different types of dark patterns that exist. The more you know about dark patterns, the easier it will be to spot them.
· Take your time when reading any terms of service or other agreements. Don't just click "agree" without reading the fine print.
· Don't be afraid to ask questions if you don't understand something. If you're not sure what a business is asking you to agree to, ask them to explain it in plain English.
· Report dark patterns to the business involved. If you see a dark pattern, you can report it to the business involved. You can also file a complaint with your local consumer protection agency.

# 05
# CONCLUSION

Dark patterns are a form of deceptive design that can harm consumers. Awareness of the different types of dark patterns and taking steps to protect your business and consumers can help to reduce risk by focusing on offering consumers the information and experience needed to make fully informed decisions.

> *Dark patterns are a form of deceptive design that can harm consumers*

# CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.



CPI COMPETITION POLICY® INTERNATIONAL