Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

November 4, 2022

What Hides in the Shadows: Deceptive Design of Dark Patterns

Many consumers have encountered "dark patterns" online, but may not recognize their name or harmful impacts. A Federal Trade Commission (FTC) staff report describes dark patterns as "design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm." Examples include (1) subscriptions that, despite all efforts, seem impossible to cancel; (2) terms and conditions hidden at the bottom of webpages in tiny fonts; and (3) buttons with confusing phrasing that result in an accidental agreement or purchase (see **Figure 1**).

Figure 1. Example of a Dark Pattern

Source: CRS, adapted from Bryce Durbin, TechCrunch.

Dark patterns are becoming increasingly pervasive online, which has raised consumer protection, privacy, and competition concerns in Congress.

Overview of Dark Patterns

Dark patterns deployed online can influence consumer behavior and decisionmaking through psychological, visual, emotional, or other tactics. Because dark patterns are often opaque and subtle, consumers may never realize the influence on their online behavior. This has led some scholars to raise concerns related to consumer autonomy, welfare, and protection. Dark patterns vary in appearance and prevalence across different industries, sites, apps, services, and contexts, so no uniform definition exists.

Dark patterns may also harm competition. Some scholars argue dark patterns are anticompetitive since they erode consumer welfare and consumer choice. For example, dark patterns may inhibit consumers from switching to other market competitors or act to decrease price transparency by limiting price comparison through bundling items or different price metrics (e.g., products are grouped together and sold as a single unit, or products use different metrics such as price per unit compared to price per ounce). Dark patterns may also influence consumer purchasing decisions (e.g., false limited-time messages or countdown timers to purchase an item) or influence users to reveal personal information. They may also make it difficult for consumers to exercise agency over their online privacy (e.g., by requiring cumbersome procedures to "opt out" of data collection). Research has found that dark patterns disproportionately affect lower-income individuals and individuals with lower levels of educational attainment.

A 2019 study found that dark patterns were present on 11% of popular e-commerce websites. Dark patterns are even more common in mobile apps: a 2020 study identified dark patterns on 95% of free Android apps in the U.S. Google Play Store. The growing prevalence of dark patterns may raise additional consumer protection concerns, especially as mobile e-commerce currently accounts for more than 70% of total e-commerce sales globally.

Types of Dark Patterns

The following represent a selection of common dark patterns:

- **Preselection:** Default selections that benefit the company (e.g., cookie consent banners that preselect to opt in to cookie tracking)
- **Nagging:** Repeated requests for certain consumer actions or denying the consumer's ability to permanently accept or decline (e.g., websites with disruptive pop-ups that continuously ask permission to send notifications)
- **Hidden Information:** Hiding important information from consumers (e.g., in lengthy terms of service or in small font)
- **Subverting Privacy:** Inducing consumers to provide more of their data than intended (e.g., online platforms that require users to provide information to gain access, or privacy settings that are difficult to utilize)

Dark patterns may also contribute to the gamification of certain online services and addiction to online platforms. Gamification refers to the use of game-like design elements and rewards systems that may give rise to impulsive decisions, often found in financial trading and educational apps. Inducing consumers to watch the next recommended video through an auto-play feature that loads new content without user action or agreement may be another example of a dark pattern. This is of particular concern for children when shown age-inappropriate content.

Advances in artificial intelligence, machine learning, and data collection and analysis techniques coupled with the use of dark patterns have raised additional concerns. Some scholars argue that companies' real-time experimentation, machine learning models, and A/B testing (which shows consumers two different versions of a user interface to allow comparison of the results) may enable and incentivize new micro-targeted dark patterns or algorithms optimized to induce specific online behavior.

Existing Oversight and Regulation

Some dark patterns may violate existing laws enforced by federal privacy and consumer protection agencies, while others may not. The Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB) have recently taken enforcement action against certain dark patterns found to be unlawful.

Federal Trade Commission (FTC)

Some dark patterns may violate Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices [UDAP] in or affecting commerce."

In recent years, the FTC has applied its existing UDAP authorities to take enforcement actions against multiple companies and online platforms that have employed dark patterns. The agency's September 2022 report, "Bringing Dark Patterns to Light," details many of these cases.

The FTC also enforces other statutes that dark patterns may violate. These include

- Restore Online Shoppers' Confidence Act, ROSCA (15 U.S.C. §§8401-8405), prohibits additional charges added after an online transaction without the consumer's express consent;
- CAN-SPAM Act (15 U.S.C. §§7701-7713), sets rules for commercial emails and allows users to opt out of emailing; and
- Children's Online Privacy Protection Act, COPPA (15 U.S.C. §§6501-6505), provides certain data protections for children under the age of 13.

However, some dark patterns may fall outside the FTC's existing authorities or require close agency examination before possible enforcement. According to the FTC's report, "there are certain dark patterns that the FTC has consistently found to be unlawful, while others would depend on a case-by-case evaluation." Limited agency time and resources may preclude the necessary evaluation of certain dark patterns.

While some scholars argue that the FTC has sufficient authorities to regulate harmful dark patterns under Section 5 of the FTC Act, others support an expansion of the agency's mandate that expressly includes "manipulative" or "abusive" practices. These critics argue the FTC's current UDAP authorities may be insufficient in cases where deception is not the core issue.

Consumer Financial Protection Bureau (CFPB)

The Consumer Financial Protection Act of 2010 (CFPA) established the CFPB as the federal government's primary regulator of consumer financial products and services. The act also gives the CFPB authority over unfair, deceptive, or abusive practices related to consumer financial products and services. The CFPB has taken enforcement action under this authority against financial service companies that allegedly abuse dark patterns. For example, in 2022, the CFPB took action against consumer credit reporting company TransUnion for employing an array of digital dark patterns in order to profit from consumers.

State Regulation

A handful of states, including California, Colorado, and Connecticut, have enacted legislation to regulate or ban certain forms of dark patterns. The California Consumer Privacy Act (CCPA) defines dark patterns as a "user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation." It is the first U.S. law to define dark patterns and served as the basis for the Colorado and Connecticut statutory definitions. The California Privacy Rights Act (CPRA), which California will begin enforcing in 2023 and expands the CCPA, includes a provision that explicitly forbids the use of dark patterns to obtain consent related to the processing of personal information.

Questions for Congress

Given the potential adverse impact of dark patterns on consumers, Congress may consider whether further action is appropriate:

- Existing data privacy and consumer protection laws prohibit some dark patterns, but not all. Congress may consider expanding the scope of those laws to address all dark patterns. For existing laws that prohibit dark patterns, limited FTC and CFPB resources may preclude fuller enforcement of those laws. Congress may consider whether relevant agencies should receive additional resources, such as from appropriations, fees, fines, or other sources to support enforcement activities.
- Congress may consider whether to address dark patterns legislatively either in broader legislation on data privacy and data protections, or in separate more targeted legislation. Some members have already introduced legislation in the 117th Congress specific to dark patterns. For example, the Deceptive Experiences to Online Users Reduction (DETOUR) Act (S. 3330) would prohibit large online platforms from using dark patterns.
- Congress may consider whether a statutory definition of dark patterns is needed, and if so, how to structure a definition or determine whether a dark pattern is unfair or deceptive. One challenge is that identification of dark patterns is often context-specific. Another is that companies might attempt to modify their techniques to circumvent statutory definitions.
- In taking any of the above approaches, Congress may consider unintended consequences, such as the risk that prohibiting dark patterns or defining legitimate consent without manipulation could limit legitimate design techniques and marketing practices.

Kristen E. Busch, Analyst in Science and Technology Policy

IF12246

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.