Alert
February 25, 2025

COZEN O'CONNOR

Unpacking Dark Patterns

"Dark patterns" have increasingly been the focus of legislative and regulatory scrutiny. Yet the phrase is never used in business. No business designs a website, mobile app, or business process with the instruction, "let's create a dark pattern." But recent state comprehensive privacy laws and regulatory actions blending privacy and consumer protection law make it clear that using a dark pattern is a legally risky action. In this article, we try to bridge the gap between the abstract concept "dark pattern" and the real world of business technology and business processes.

What Are Dark Patterns?

At a high level, dark patterns are user interface and user experience designs that mislead or coerce users, that manipulate a user's behavior to cause a result the user did not intend, or that impair a user's ability to make an informed decision. However, each statute and regulator has its own definition of what a dark pattern is, and here we start to see the intersection of privacy laws and traditional consumer protection concepts.

Examples of dark patterns include:

- Making it difficult to cancel subscriptions;
- Displaying extra fees only at checkout;
- Tricking users into sharing more personal data than they intended;
- Guilt-tripping users into opting in; and
- Highlighting irrelevant information to distract users from important details.

Federal Trade Commission

In its staff report, *Bringing Dark Patterns to Light* (available here), the Federal Trade Commission (FTC) defines "dark patterns" as design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm. These manipulative design techniques often take advantage of consumers' cognitive biases to steer their conduct or delay access to information needed to make fully informed decisions. If the FTC believes a company has engaged in deceptive trade practices, it can initiate administrative proceedings against the company, impose civil fines, and seek temporary and permanent injunctions from courts, among other remedies. *Bringing Dark Patterns to Light* includes the following examples of digital dark patterns, which the FTC views as deceptive trade practices. Below are a list of types and examples.

Endorsements/Social Proof

- False Activity Messages — Making false claims about activity on a site or interest in a product (such as "33 other people are using this site").
- Deceptive Consumer Testimonials — using false customer endorsements or omitting material information about other people's experiences, such as the endorsers were compensated or the endorsers have a connection to the company.
- Deceptive Celebrity Endorsements — featuring celebrities or influencers to endorse a product without disclosing that they were paid for the endorsement or were given the product for free.
- Parasocial Relationship Pressure — using characters that children know and trust to pressure them into making a certain choice.

Scarcity

- False Low Stock Message — creating pressure to buy immediately by saying inventory is low when it isn't, such as "Only 1 left in stock – order soon."

Andrew Baer

Chair, Technology, Privacy & Data Security

abaer@cozen.com
Phone: (215) 665-2185
Fax: (215) 372-2400

Christopher Dodson

Member

cdodson@cozen.com
Phone: (215) 665-2174
Fax: (215) 372-2408

Related Practice Areas

- Business
- Technology, Privacy & Data Security

- False High Demand Message — creating pressure to buy immediately by saying demand is high when it isn't, such as "18 other shoppers have this item in their carts."

Urgency

- Baseless Countdown Timer — creating pressure to buy immediately by showing a fake countdown clock that just goes away or resets when it times out, such as "Offer ends in 00:59:48."
- False Limited Time Message — creating pressure to buy immediately by saying the offer is good only for a limited time or that the deal ends soon — but without a deadline or with a meaningless deadline that just resets when reached.
- False Discount Claims — creating pressure to buy immediately by offering a fake "discounted" or "sale" price.

Obstruction

- Price Comparison Prevention — preventing shoppers from easily comparing prices by bundling products, using different measures (price per unit vs. price per ounce), or listing the price per payment (such as $10 per week) without disclosing the total number of payments or overall cost.
- Roadblocks to Cancellation — making it easy to sign up but hard to cancel, by requiring people to go through tedious, time-consuming cancellation procedures.
- Immortal Accounts — making it hard or impossible to delete an account.

Sneaking or Information Hiding

- Sneak-into-Basket — automatically adding items to the shopping cart without a shopper's permission; or tricking a shopper into buying unwanted items by using a pre-checked box.
- Hidden Information — hiding material information or significant product limitations.
- Hidden Costs — adding hidden fees or other charges.
- Drip Pricing — advertising only part of a product's total price initially and then imposing other mandatory charges late in the buying process, such as a "convenience fee" that appears only when a shopper reaches the check-out screen.
- Hidden Subscription or Forced Continuity — offering a free trial and, at the end of the trial, automatically and unexpectedly charging a recurring fee if consumers don't affirmatively cancel; or offering a product for a small one-time fee, then automatically enrolling people into a subscription or continuity plan without consent.
- Intermediate Currency — Hiding the real cost by requiring consumers to buy things with virtual currency.

Interface Interference

- Misdirection — using style and design to focus users' attention on one thing in order to distract their attention from another, such as presenting the subtotal price in a bright green highlighted box, then listing additional mandatory taxes and fees below in a non-highlighted section so users don't notice their final total will be higher.
- False Hierarchy or Pressured Upselling — using contrasting visual prominence to steer users into making a certain selection, such as during cancellation presenting the "Keep My Subscription" option as a bright orange button, while presenting the "Cancel My Subscription" option as a smaller font, pale gray hyperlink hidden below the orange button.
- Disguised Ads — formatting advertisements to falsely appear to be unbiased product reviews or independent journalism; or presenting a ranking list, search engine, or comparison shopping site as neutral and unbiased when it is actually based on paid advertising.
- Bait and Switch — a choice or interaction leads to an unexpected, undesirable outcome, such as a user clicks the X in the top right corner of a pop-up but, instead of closing the box, it downloads software, or selling a consumer something that turns out to be materially different than what was originally advertised.

Coerced Action

- Unauthorized Transactions — tricking people into paying for goods or services that they did not want or intend to buy, such as mislabeling the steps in a transaction or failing to obtain the express informed consent of the accountholder, such as a shopping website button labeled "Next" that people think will lead to the next screen but, instead, processes the transaction immediately, or a one-click button in children's gaming apps that charges parents real money.

- Auto-Play — automatically playing another video once one video ends in a manner that is unexpected or harmful, such as if after the first video, a less kid-friendly video — or a sponsored ad camouflaged to look like a recommended video — automatically plays.
- Nagging — asking repeatedly in a disruptive manner if a user wants to take an action, or making a request that doesn't let the user permanently decline and then repeatedly prompting them with the request, such as asking users to provide their data or turn on cookies and then repeatedly presenting the choices as "Yes" or "Not Now" instead of "Yes" or "No."
- Forced Registration or Enrollment — making users create an account or share their information to complete a task, such as "Create an account to continue with your purchase."
- Pay-to-Play or Grinding — saying that things are available with a purchase or download, but then charging users to actually obtain those things; or making the free version of a service or game so cumbersome and labor-intensive that the user is induced to unlock new features with in-app purchases.
- Friend Spam, Social Pyramid Schemes, and Address Book Leeching — asking for an email address or social media permissions for one purpose but then using them for another; or making users share information about people in their social network.

Asymmetric Choice

- Trick Questions — using ambiguity or confusing language — often double negatives — to steer a user to things they don't want, such as "Uncheck the box if you prefer not to receive email updates"; or a checkbox next to the phrase "Decline the option of renewing your loan," which if left un-checked is interpreted as acceptance of auto-renewal terms; or when trying to cancel a subscription service, a button labeled "No, cancel" that doesn't cancel your subscription but instead takes you out of the cancellation path.
- Confirm Shaming — using shame to steer users away from certain choices by framing the alternatives as a bad decision, such as if "No, I don't want to save money" appears when a shopper selects a one-time purchase over a recurring one.
- Preselection — preselecting a default that's good for the company, but not the user, such as if add-on products like trip insurance or an extended warranty are automatically tacked on to a purchase unless the customer notices and opts out; the "accept" tracking cookies box is prechecked; or the site automatically shows shoppers the most expensive option, not the cheaper or free option.
- Subverting Privacy Preferences — tricking users into sharing more information than they really intended to, such as asking users to give consent but not informing them in a clear, understandable way what they are agreeing to share, or telling users the site is collecting their information for one purpose but then sharing it with others or using it for other purposes, or including default settings that maximize data collection and making it difficult for users to find and change them, or giving users a choice, but one where the "Accept" choice is in a bold, blue background, while "Reject" is greyed out and in small print.

GDPR

The European Union General Data Protection Regulation (GDPR) does not explicitly address dark patterns. However, under the GDPR, all processing of personal data must be fair and transparent, which the use of dark patterns is not. The European Data Protection Board (EDPB), the EU-wide privacy regulator that enforces the GDPR in consultation with the national supervisory authorities, has provided guidance on dark patterns in the context of social media platforms, the principles of which apply beyond social media platforms.

The EDPB describes dark patterns as user interfaces and user experiences that attempt to influence users into making unintended, unwilling, and potentially harmful decisions, often where an action is favorable to the designer's interests and not the users' interests. The EDPB describes six categories of dark patterns. In addition to providing a private right of action for data subjects, the GDPR empowers the EU supervisory authorities to initiate administrative proceedings and issue fines for violations of the GDPR. Fines for violating the GDPR can be as high as the greater of 20 million euros or 4% of global revenue.

Overloading

- Confronting users with a large quantity of requests, information, options, or possibilities in order to prompt them to share more data or unintentionally allow personal data processing against the expectations of the data subjects.

Skipping

- The user interface or user experience is designed in a way that users forget or do not think about all or some of the data protection implications.

Stirring

- The user interface or user experience affects the choice users would make by appealing to their emotions or using visual nudges.

Obstructing

- Interfering with users from becoming informed or managing their data by making the action hard or impossible to achieve.

Fickle

- An inconsistent or unclear clear user interface that makes it hard for users to understand the different data protection control tools or to understand the purpose of the personal data processing.

Left in the Dark

- Information or data protection control tools are hidden or leave users unsure of how their personal data is processed and what control they might have over it.

State Comprehensive Privacy Laws

A more recent entry into the legal arena is the presence of dark pattern restrictions in U.S. state comprehensive privacy laws. The comprehensive privacy laws in California, Colorado, Connecticut, Delaware, Florida, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Rhode Island, and Texas regulate dark patterns. Only Indiana, Iowa, Kentucky, Tennessee, Utah, and Virginia passed on the opportunity to explicitly address dark patterns in their respective comprehensive privacy laws.

All states regulating the use of dark patterns through their comprehensive privacy laws take one of two approaches. California, Colorado, Minnesota, and Montana define a "dark pattern" as a user interface designed with the substantial effect of subverting or impairing user autonomy, decision-making, or choice. Connecticut, Delaware, Florida, Maryland, Nebraska, New Hampshire, New Jersey, Rhode Island, and Texas start with the same definition but also include any practice that the FTC refers to as a "dark pattern." Each of the states regulating dark patterns specifies that consent for privacy purposes does not include agreement obtained through the use of dark patterns.

At present none of the comprehensive state privacy laws includes a private right of action for the use of dark patterns so enforcement is by the state's attorney general or the state's privacy regulator in California. Many states impose civil penalties of up to $7,500 per violation but some, such as Connecticut and Florida, are as high was $50,000 per violation.

State Consumer Protection Law

Additionally, every U.S. state has a consumer protection law prohibiting unfair or deceptive practices (UDAP). Many state attorneys general treat dark patterns as a UDAP violation. Furthermore, consumers have a private right of action under state consumer protection laws. So companies using dark patterns could leave themselves exposed to actions from state attorneys general as well as private consumers.

Best Practices

We have described in detail what not to do. But what are some best practices for avoiding dark patterns?

From the FTC's guidance, we can distill a number of best practices.

Transparency and Clear Disclosures

- Ensure that all material information is clearly and conspicuously disclosed to consumers.
- Avoid hiding key terms in dense terms of service documents or behind hyperlinks.

Express Informed Consent

- Ensure that consent involves an affirmative, unambiguous act by the consumer.

Simple Cancellation Mechanisms

- Provide cancellation mechanisms that are as easy to use as the method used to sign up.
- Avoid subjecting consumers to unreasonable delays or additional offers when they attempt to cancel.

Avoiding Deceptive or Manipulative Design Techniques

- Do not use design techniques or elements that induce false beliefs or hide material information or manipulate consumers into making choices they would not otherwise make, such as making rankings appear objective when compensation was paid to be included in the rankings.
- Ensure that advertisements and promotional messages are clearly identified as such.

Respecting Privacy Choices

- Make privacy choices easy to access and understand.
- Avoid default settings that lead to unexpected data collection, use, or disclosure.

Avoiding Deceptive or Unauthorized Charges

- Obtain consumers' express informed consent before charging them for goods or services.
- Ensure that any unavoidable and mandatory fees are included in the upfront, advertised price.
- Do not trick consumers into paying for goods or services they did not intend to buy.
- Ensure that any free trial offers clearly disclose the terms and conditions, including any automatic charges after the trial period.

The EDPB is more specific and more granular in its recommendations for best practices in the privacy arena.

Shortcuts

- Provide links, wherever users encounter related information, to settings or information that helps users manage their data and data protection settings.

Bulk Options

- Group options or settings with the same processing purpose together, allowing users to change them all at once while still offering a way to make granular changes to the options or settings.

Contact Information

- Clearly state, in a section where users expect to find it, the company's contact address for addressing data protection requests in the privacy policy.

Reaching the Supervisory Authority

- Include the identity of the supervisory authority and a link to its website or the specific page for lodging a complaint in a section where users expect to find it.

Privacy Policy Overview

- At the start of the privacy policy, include a collapsible table of contents with headings and sub-headings that show the different passages the privacy policy contains.

Change Spotting and Comparison

- When changes are made to the privacy notice, make previous versions accessible with the date of release and highlight changes.

Consistent Wording

- Use the same wording and definitions across the website, including the privacy policy, for the same data protection elements.

Providing Definitions

- When using unfamiliar or technical words or jargon, provide a definition in plain language to help users understand the information.

Contrasting Data Protection Elements

- Make data protection-related elements or actions stand out visually in an interface.

Data Protection Onboarding

- Include data protection information as part of the onboarding experience for users and invite users to set their data protection preferences.

Use of Examples

- Clearly and precisely state the purpose of processing; use examples to illustrate specific data processing to make it more tangible for users.

Sticky Navigation

- While consulting a page related to data protection, keep the table of contents constantly displayed on the screen, allowing users to always situate themselves on the page and quickly navigate the content using anchor links.

Back to Top

- Include a return to top button at the bottom of the page or as a sticky element at the bottom of the window to facilitate users' navigation on a page.

Notifications

- When a user makes changes to settings, use notifications to raise awareness of the risks related to personal data processing, such as through inbox messages, pop-in windows, or fixed banners at the top of a webpage.

Explaining Consequences

- When users want to activate or deactivate a data protection control, or give or withdraw their consent, inform them in a neutral way about the consequences of such action.

Cross-Device Consistency

- Ensure settings and information related to data protection are located in the same spaces across different platforms (such as computers or mobile apps) and are accessible through the same user interface and user experience elements (such as menus or icons).

Data Protection Directory

- Provide users with an easily accessible page from where all data protection-related actions and information are accessible.

Contextual Information

- In addition to an exhaustive privacy policy, provide short bits of information at the most appropriate time for the user to have specific and continuous information on how their data are processed.

Self-Explanatory URL

- Use web addresses that clearly reflect the content of pages related to data protection settings or information, such as [url.com]/data-settings.

Exercise of the Rights Form

- Provide a dedicated form to assist users in exercising their data subject rights, helping them understand their rights and guiding them in carrying out these requests.

- These best practices aim to create a transparent, user-friendly interface that respects users' data protection rights and helps them make informed decisions about their personal data.

Conclusion

Legislators and regulators are highlighting concerns about dark patterns, making it important for businesses to proactively adjust their user experience designs. By prioritizing transparency and fairness, organizations can enhance trust, avoid penalties, and stay ahead of an evolving regulatory landscape.