Hashed & Salted | A Privacy and Data Security Update
November 2022

If You Don't Read This Article About Dark Patterns, You're Missing the Opportunity of a Lifetime

How many times has this happened to you? You get a pop-up that guilts you into providing an email address to sign up and save ("No, I like paying full price."). Or the highlighted button to move forward in a selection actually sends you back to the previous screen. Or a box is prechecked to opt you in to marketing. Or you notice that a warranty extension has been added to your cart without your request.

These are examples of dark patterns—user interfaces designed to manipulate consumers to keep them from opting out of their intended choice.

In the past few years, regulators around the United States (and the EU) have ramped up efforts to discourage and prosecute such practices. Recently, both the Federal Trade Commission (FTC) and the California Privacy Protection Agency (CPPA) have issued reports and regulations, respectively, that outline how to identify dark patterns as well as the penalties associated with utilizing dark patterns in web-based commerce. There also have been several lawsuits and litigation surrounding the use of dark patterns as deceptive and unfair practices.

This article clarifies how to identify dark patterns and provides advice on how to avoid introducing dark patterns into the user experience.

Common Dark Patterns

Below are some of the common dark patterns:

- Design elements that induce false beliefs—for example, advertising disguised as editorial content, messaging that "shames" someone for their choice (e.g., someone who declines to provide an email in exchange for a coupon is told "You must hate your money!") or urgent claims that suggest an item is almost sold out when it isn't.
- Design elements that hide material information—for example, obscured prices, bait-and-switch tactics that lure a user with one outcome/price but something else happens or burying charges in blocks of text.
- Design elements that lead to unauthorized charges—for example, trial services that charge you automatically when the trial expires; items that are snuck into a basket; misdirection, where the design nudges users toward a more expensive option; or making it difficult to cancel a service or a subscription.
- Design elements that obscure privacy choices—for example, repeated prompts to share data, and prechecked boxes or double negatives to confuse the consumer making a choice.

Laws Regulating Dark Patterns

There are several federal and state laws regulators can enforce against websites employing dark patterns. First, the FTC can (and does) prosecute organizations under their Section 5 authority for unfair and deceptive trade practices. Second, state attorneys general (AGs) and consumers can bring actions against businesses under their state's unfair and deceptive trade practices (UDAP) law. Finally, a few states have passed privacy laws that address dark patterns.

Attorney Advertising

FTC and State UDAP Laws

Under Section 5 of the FTC Act, the FTC can combat unfair and deceptive practices. The FTC has defined an unfair trade practice as one that causes or is likely to cause a substantial injury, is not outweighed by any countervailing benefits to consumers or competition, and causes an injury that consumers could not have reasonably avoided. A deceptive trade practice is a material practice that is likely to mislead consumers acting reasonably under the circumstances. Recently, the FTC has brought actions against companies for the following types of dark patterns:

- Emails sent to consumers falsely claimed they were coming from news sites. When a user clicked on them, they were ultimately routed to a sales website, resulting in a settlement of $1.5 million.
- Fees were hidden in Lending Club's loan application and required scrolling to be visible, resulting in a settlement of $18 million.
- ABC Mouse failed to tell users that the membership would continue indefinitely, and canceling a membership required a user to navigate six to nine screens. Multiple buttons displayed that would remove the user from the cancellation experience, resulting in a settlement of $10 million.
- Vizio had a default setting turned on that collected TV viewing data and shared the data with third parties resulting in a settlement of $2.2 million.

In its recent workshop and report, the FTC has said that it plans to ramp up its enforcement against dark patterns. Additionally, state AGs and class action plaintiffs have brought UDAP cases against businesses utilizing dark patterns. These lawsuits have resulted in even higher settlements or verdicts. For example, Vizio was also sued by class action plaintiffs for the same covert collection of viewing data, resulting in a settlement of $17 million. Noom agreed to pay $56 million and provide $6 million in subscription credits to settle a lawsuit alleging that they failed to disclose that the trial period would extend indefinitely and that they had barriers to cancellation, including requiring consumers to cancel through a virtual coach.

California Privacy Rights Act, Colorado Privacy Act, and Connecticut Data Privacy Act

CAs of now, three states' privacy statutes also have regulations relating to the use of dark patterns in obtaining consent from consumers: the California Privacy Rights Act (CPRA), Colorado Privacy Act (CPA) and Connecticut Data Privacy Act (CDPA).

CPRA. The CPRA specifically prohibits the use of dark patterns to obtain consent for privacy-related choices. The CPRA defines a dark pattern as a "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy." Draft regulations released by the CPPA explain that businesses should avoid architectures that interfere with the consumer's ability to choose, "because consent must be freely given, specific, informed, and unambiguous." Critically, the regulations explain that while a business's intent for its user experience is a factor in determining the existence of a dark pattern, it is not dispositive. A business that chooses to ignore the existence of a dark pattern in its user interface can still be held liable for it.

The draft regulations provide some relevant examples of what may constitute a dark pattern:

- Language that is difficult to understand or confusing (e.g., using double negatives or unintuitive placement of buttons).
- Asymmetrical privacy choices, such as requiring more steps to opt out of sharing personal information in comparison to opting in or banners that provide unequal choices (e.g., "Accept all cookies" and "Preferences").
- Manipulative language, such as requiring consumers to click through disruptive screens before opting out of sharing personal information or bundling privacy choices such that a consumer is required to agree to share personal information for an unexpected use (e.g., requiring a consumer to share location services both for finding nearby restaurants and sharing precise geolocation with data brokers).
- Difficult or impossible to submit data subject requests(e.g., broken links or unmonitored inboxes).

Businesses must consider five measures to avoid dark patterns in their web and app interfaces. Those include ease in use of language, ensuring that the same amount of time is required to choose a more privacy-protective option as it does to choose the less privacy-protective one, avoiding elements and language that are confusing, avoiding manipulative language, and ease of execution to submit a data subject access request.

CPA and CDPA. The CPA and CDPA also prohibit the use of dark patterns in obtaining consent—using an almost identical definition of a dark pattern. Critically, since the CPA requires consumers to opt in to the collection of sensitive information (unlike the CPRA and CDPA, which just require consumers to be able to opt out of the collection of sensitive personal information), avoiding dark patterns in obtaining consent is even more critical.

Major Takeaways

Website and app designers should consider adopting a "privacy by design" framework for their user experiences and avoiding any appearance of manipulation. Below are some recommendations for designing (or even modifying) your user experience to avoid dark patterns:

- Make clear whether the content is an advertisement.
- Be upfront with any costs or fees.
- Make it easy for consumers to unsubscribe or cancel a trial.
- Do not preselect choices, but especially avoid preselecting choices that eliminate privacy rights.
- Avoid language that shames consumers for exercising their rights.
- Do not make unsubstantiated claims.
- Make sure that users can easily exercise their privacy rights.
- Avoid posing double negatives or trick questions to consumers.
- Make the user experience intuitive.

Related Professionals

Daniela Spencer . . . . . dspencer@loeb.com
Jessica B. Lee . . . . . jblee@loeb.com

7120 REV1 11-08-2022