Proskauer

FTC Workshop: “Bringing Dark Patterns to Light”

Proskauer on Advertising Law Blog on **May 5, 2021**

The FTC recently held a workshop titled “Bringing Dark Patterns to Light,” a recording of which can be found at the following link. The workshop centered around exploring the effects of digital “dark patterns” on consumers and the marketplace.

The term “dark patterns” refers to a range of potentially deceptive website design tactics that can manipulate consumers’ behavior or limit their autonomy. Dark patterns can deceive consumers into purchasing, sharing, or agreeing to items consumers did not intend to purchase, share, or agree to. Dark patterns are also employed to make it confusing or difficult to terminate agreements or subscriptions. Increasingly, companies are also using dark patterns to manipulate consumers into giving up their personal data, which is sold and then used to target advertising and manipulate future behavior.

Some examples of “dark patterns” include:

- a website that automatically adds items to a user’s online shopping cart;
- the “bait and switch,” where a user looking to take one course of action is redirected to a completely unforeseen result. For example, if pressing an “X” at the top right corner of a pop-up – which normally results in closing the window – actually initiates a download;
- “disguised ads” designed to blend in with other content or navigation on the page, to manipulate consumers into clicking on them.

Panel 1: “What are Dark Patterns, and Why Are They Employed?”

One FTC workshop panel focused on defining dark patterns and identifying the drivers of dark patterns.

According to the panelists, dark patterns have one of six attributes – they 1) are deceptive, 2) constitute “information hype”, 3) are asymmetric, 4) are covert, 5) result in differential treating, or 6) are restrictive.

- “Deceptive” dark patterns induce false beliefs — for example, a countdown timer that does not relate to what is being advertised, meant to mislead consumers into believing the availability of items or discounts are time-limited.
- “Information hype” dark patterns delay or hide important information from users – for example, hidden fees shown only after the user has spent time selecting items.
- “Asymmetric” dark patterns make it hard to access certain choices that disadvantage the advertiser. A common example is where websites hide the option to decline consent to cookies (while making the “accept” option readily accessible).
- “Covert” dark patterns manipulate users without their knowledge. For example, where a pop-up asks for a consumer’s email address and phone number in exchange for a discount, even though (unbeknownst to most consumers) only one piece of information is required for the discount.
- “Differential treating” dark patterns disadvantage and treat one group of users differently from another – for example, where the only way to get ahead in a video game is to purchase features and not by your own skill (thereby treating users who have the means and willingness to pay differently from those who do not).
- “Restrictive” dark patterns eliminate certain options from user interfaces altogether – for example, to sign up for a service, a consumer must agree to both the terms and conditions *and* marketing emails to proceed.

While unique in their own ways, the panelists noted that dark patterns ultimately function in two ways: (1) by manipulating information flow to users or (2) by modifying the decision space for users and ultimately influencing how users make choices.

A study by one of the panelists demonstrated how and how often a consumer experiences dark patterns depends on the consumer’s preferred interface. According to this study, use of dark patterns and the variety of dark patterns employed is higher on apps than on mobile or desktop websites. While this may be due to many factors, the panelist believed it demonstrates how important it is to understand that a review of a website on one interface or platform might not provide a complete and accurate picture of an advertiser’s use of dark patterns.

Panel 5: “How Can We Best Continue to Address Dark Patterns?: Potential Strategies for Dealing with Dark Patterns”

In another workshop, panelists discussed the current legal regime and enforcement challenges related to dark patterns, how to prioritize efforts to combat dark patterns, and various solutions for mitigating the harmful effects of dark patterns on consumers. Notable members of this panel include Laura Brett, director of the NAD, and Jennifer Rimm, an Assistant Attorney General of the Office of Consumer Protection at the Office of the Attorney General for the District of Columbia.

The panel noted there has recently been an increased interest in regulating dark patterns. The FTC is actively working to combat these unfair practices by bringing enforcement actions under the FTCA and statutes such as the Restore Online Shoppers Confidence Act, which requires sellers of subscription plans to disclose all material terms and provide a simple way to cancel. Policymakers have also expressed willingness to prohibit dark patterns in impending and recently-enacted privacy legislation. The California Consumer Privacy Act, which went into effect in 2020, was the first privacy law to specifically prohibit dark patterns in opt-out processes. The Act gives consumers the right to stop, access, and delete the sale of their online information, and prevents advertisers from using processes intended to impair a consumer's choice to opt out.

Federal courts of appeals have also backed the FTC in cases alleging that dark patterns were used to deceive consumers. For example, the Second Circuit in *FTC v. LeadClick Media* found the defendant's website, which sold colon cleanses and weight loss products, violated the FTC Act where it included fake customer testimonials drafted by the company and advertising content that was designed to look like independent journalism.

State Attorneys General have also recently brought consumer protection cases involving dark patterns. One such case was brought against Instacart in the District of Columbia for adding a 10% default charge allegedly designed to look like a tip for the driver, when in fact it was collected by Instacart. A similar suit, currently ongoing in the District of Columbia, was brought against Marriot Hotels for not including a mandatory amenity and resort fee in the advertised price of its hotel rooms, and for using a number of other allegedly deceptive design strategies that obscured the fee.

The panel also noted the potential for independent self-regulation, including NAD, to help deter dark patterns. One panelist noted that – as with other marketing practices – robust FTC enforcement promotes better self-regulation; strong FTC enforcement motivates advertisers to comply with NAD recommendations, and to bring NAD challenges against competitors who use unfair practices to tilt the competitive landscape in their favor.

Advertisers should be cognizant that the use of dark patterns exposes them to the risk of FTC enforcement actions, NAD challenges, and other legal liabilities. In addition to these legal risks, once exposed, dark patterns can quickly erode consumer trust and company goodwill, leading to long-term losses. Steps advertisers should take to avoid engaging in practices that could be viewed as dark patterns advertisers include:

- Making sure options to cancel subscriptions are not hidden.
- Avoiding practices that would surprise a consumer. Such practices to avoid include:
  - automatically adding items to a user's purchase basket without a customer's consent;
  - concealing unexpected charges;
  - disguising advertisements as part of regular content.

To the extent online platforms use AI systems as part of the design process or to generate marketing materials, advertisers should also proactively review the material to ensure the absence of dark patterns.

View Original

Related Professionals

- **Baldassare Vinti**
  Partner
- **Jennifer Yang**
  Partner
- **Nicole Sockett**
  Associate
- **Jessica M. Griffith**
  Associate