FTC Renews Focus on Digital Dark Patterns With Release of New Staff Report

Authors: Jamie Haddad and Frank Gorman

The Federal Trade Commission ("FTC") issued a report in September analyzing digital "dark patterns," which are deceptive design practices that "trick or manipulate consumers into buying products or services or giving up their privacy."[1] The report comes nearly a year after the agency published an enforcement policy statement on the topic and seeks to renew the agency's position against dark pattern tactics.

The full report (including Appendices) details over 30 practices that raise consumer protection concerns. It also analyzes recent FTC cases that have challenged allegedly illegal dark patterns and makes recommendations to companies on how to develop, design, and improve their online interfaces. Here are the four main tactics highlighted in the report:

Design Elements that Induce False Beliefs
A common example of this tactic is the use of advertisements deceptively formatted to look like independent news articles to entice consumers to buy certain products. Other examples include purportedly neutral comparison-shopping sites that actually rank companies based on compensation, false claims of scarcity, and fake countdown timers.

Design Elements that Hide or Delay Disclosure of Material Information
This type of dark pattern involves burying key terms of a product or service within dense text, like the Terms of Service, that consumers are unlikely to read before purchase. It also includes hiding material information "below the fold" on standard screen configurations or "drip pricing," in which companies advertise only a part of a product's total price to lure in customers and do not mention other mandatory charges until later in the transaction.

Design Elements that Lead to Unauthorized Charges
This category includes tactics that trick consumers into paying for goods or services they did not intend to, often on a recurring basis. This often occurs when the material terms of the transaction are not clearly disclosed or the subscriptions are difficult to cancel.

Design Elements that Obscure or Subvert Privacy Choices
These manipulative tactics appear to give consumers a choice about sharing data, but then intentionally steer them to the option that gives away the most personal information. Examples include not allowing consumers to definitively reject data collection, repeatedly prompting consumers until they acquiesce and select the setting they wish to avoid, purposely obscuring certain privacy choices or making them difficult to access, highlighting a choice that results in more information collection while greying out the option that enables consumers to limit such practices, and including default settings that maximize data collection and sharing.

[1] *FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers*, FTC (Sept. 15, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers; *FTC Issues Illuminating Report on Digital Dark Patterns*, FTC (Sept. 19, 2022), https://www.ftc.gov/business-guidance/blog/2022/09/ftc-issues-illuminating-report-digital-dark-patterns.

Overall, the report is clear: this administration means business and web-based commerce companies should heed its warning. The digital booby traps must go.