Suits Against Google Signal Increased 'Dark Patterns' Scrutiny

By **Michele Aronson, Colleen Brown and Benjamin Mundel** (June 15, 2022)

Michele Aronson

Colleen Brown

Benjamin Mundel

Pending lawsuits against Google LLC illustrate how regulators and plaintiffs lawyers are increasingly wielding a dark patterns theory in challenging companies' practices involving consumers.

The attorneys general of Washington, D.C., Washington state, Texas and Indiana all filed complaints against Google, alleging that the company tricks consumers into providing their location data, on Jan. 24.

The cases are State of Texas v. Google LLC, in Victoria County District Court; State of Washington v. Google LLC, in King County Superior Court; State of Indiana v. Google LLC, in Marion County Superior Court; and District of Columbia v. Google LLC, in the Superior Court of the District of Columbia.

These recent lawsuits are another example of the trend of multistate attorney general and Federal Trade Commission investigations shaping privacy law and public policy in the absence of comprehensive federal legislation. Not only do these lawsuits highlight how state attorneys general are taking a more active role in challenging tech giants, but they also shed light on the types of lawsuits that consumer-facing companies of all sizes can expect in the future.

The FTC and state attorneys general have long brought lawsuits to enjoin unfair and deceptive practices, pursuant to Section 5 of the FTC Act and state consumer protection statutes. But it is only in the past few years that regulators have argued that the use of dark patterns may constitute a violation under those laws.

Indeed, the recent lawsuits against Google are the first time high-profile state enforcement actions have explicitly invoked dark patterns.

Dark patterns are design tricks that manipulate behavior in a way that is harmful to the consumer. This term has entered the privacy lexicon as privacy advocates and regulators express growing concern over companies influencing their users' online decisions.

The concept originated in academia about a decade ago, and goes to the heart of the liberty interest protected by privacy law and regulation. It is now gaining traction with regulators, legislators and litigants.

Early discussion around dark patterns queried whether the FTC and other regulators required new authorities to specifically target dark patterns. But the FTC has called upon both the "unfair" and "deception" prongs of its existing authorities under Section 5 of the FTC Act to bring actions against dark pattern practices, and has repeatedly asserted that no new legislation is required.

The unfair authority requires the FTC to establish that the practice causes substantial injury to consumers that cannot reasonably be avoided by consumers, and is not outweighed by countervailing benefits. The deception authority requires the FTC to establish that there is a material misrepresentation, omission or practice that is likely to mislead a consumer acting unreasonably under the circumstances.

In April 2021, the FTC held a workshop to examine digital dark patterns,[1] and in October 2021, announced its plans to increase its dark patterns enforcement.[2]

Class action litigators have similarly taken notice of dark patterns, and in the past few years have asserted claims such as fraud, breach of contract, and violation of state unfair competition and consumer protection laws based on alleged uses of dark patterns, including tricking users into signing up for recurring bills or maintaining subscriptions through complex cancellation procedures.

Nevertheless, serious questions remain about whether certain practices — some of them common and long-standing advertising practices — should be considered dark patterns. To that end, federal and state legislators have begun to incorporate prohibitions on dark patterns into draft legislation.

Federal legislation first proposed in 2019 and reintroduced in December 2021, the Deceptive Experiences to Online Users Reduction Act, would prohibit large online platforms from using dark patterns. The California Privacy Rights Act and the Colorado Privacy Act, which both take effect in 2023, provide that consent based on dark patterns is not valid.

While there are emerging definitions,[3] the broad and flexible concept may well sweep in a host of everyday business activities not necessarily closely monitored by legal and compliance departments. The fluidity of the concept and lack of clear regulatory guidance informed by notice and comment rulemaking thus present an expansive legal risk.

The latest lawsuits against Google, one of which has already survived a motion to dismiss, demonstrate the enhanced scrutiny being given to dark patterns, and they foreshadow an increased reliance on dark patterns theories in future litigation. There will likely be even more litigation that explicitly relies on dark patterns claims — in the form of both Section 5 lawsuits brought by the FTC, and state consumer protection lawsuits brought by state regulators and class action plaintiffs.

This issue affects companies of all sizes, and extends to consumer-facing companies in all industries that have any type of digital presence. For example, the FTC has emphasized that it will scrutinize any company that makes it difficult for consumers to cancel their subscription digitally.

Privacy- and consumer-conscious businesses should take note of the lawsuits, and do their best to ensure that their current and future practices do not put them at risk of dark patterns enforcement. Consumer-facing companies should work with counsel to develop policies that guide decisions relating to marketing and other consumer-facing interactions based on this quickly evolving body of dark patterns law.

Companies should review existing and new websites and product campaigns to ensure that their design interfaces — online and offline — do not deceive or manipulate consumers. Businesses should be particularly transparent with consumers about how their personal data, including location data and other sensitive data, is collected, used and shared.

Businesses should also evaluate any tactics or designs that may be considered to manipulate consumer choices, or that fail to disclose their practices to consumers. This includes scrutiny of privacy choices, such as data collection and usage practices, as well as commercial choices like auto-renewals.

Failure to do so may not only undermine a company's reputation with its customers, but also create significant litigation and regulatory risk, as dark patterns claims are certain to proliferate in the coming months and years.

Michele Aronson is a managing associate, and Colleen Brown and Benjamin Mundel are partners, at Sidley Austin LLP.

Josh Fougere, a partner at the firm, contributed to this article.

[1] https://www.ftc.gov/news-events/events-calendar/bringing-dark-patterns-light-ftc-workshop.

[2] https://www.ftc.gov/news-events/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap.

[3] The CPRA and CPA both define a "dark pattern" as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice." Cal. Civ. Code §1798.140(l); C.R.S. §6-1-1303(9). Similarly, the proposed DETOUR Act would make it unlawful for any large online operator "to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data." DETOUR Act, S. 3330, 117th Cong. § 3(a) (2021).