Law360

How Cos. Can Ease Risk Amid 'Dark Pattern' Regulatory Focus

By **Elizabeth McGinn, Sherry-Maria Safchuk and Melina Montellanos** (January 17, 2023)

Elizabeth McGinn

Sherry-Maria Safchuk

Melina Montellanos

Federal and state regulators, legislators, and courts have increased their focus on dark patterns — web and mobile design elements that shepherd users to make decisions, often not in their best interest.

To avoid consumer dissatisfaction, as well as legal and regulatory risk, companies should consider proactively reviewing their online activity and communications to ensure their websites and mobile applications are clear, easy to understand, and do not include deceptive or confusing design features.

Identifying Dark Patterns

The industry has not settled on one definition of what is considered a dark pattern. However, certain regulators have provided some clarity on what they consider to be covered by the term.

For example, the Federal Trade Commission defines dark patterns as "design features used to deceive, steer, or manipulate users into behavior that is profitable for an online service, but often harmful to users or contrary to their intent."

The Consumer Financial Protection Bureau similarly has defined the term as "hidden tricks or trapdoors companies build into their websites to get consumers to inadvertently click links, sign up for subscriptions, or purchase products or services."

At the state level, the California Consumer Privacy Act, as amended by the California Privacy Rights Act and effective Jan. 1, defines "dark pattern" as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation."

Examples of dark patterns include making it difficult for consumers to cancel a subscription service, revealing previously undisclosed fees right before a purchase is made, and using confusing language or visual interferences to prevent the consumer from understanding the terms of a service or from selecting a particular option.[1]

State and Federal Scrutiny

While the specific term dark pattern is a fairly new one, for more than two decades courts have reviewed whether online contracts were entered into through deceptive, manipulative or unfair ways, rendering the online agreement unenforceable.

Recently, regulators have stepped up their enforcement efforts, and both federal and state legislators are addressing their concerns through legislation.

Federal Regulators

The CFPB has brought enforcement actions against companies allegedly using dark patterns under the theory that those practices are unfair, deceptive, or abusive acts or practices, and in violation of the Consumer Financial Protection Act.

In October, the CFPB filed a complaint against an online event registration and payments processing company for, among other things, allegedly failing to disclose that consumers were signing up for an annual subscription discount club when they were simply trying to sign up for fundraising road races and other events.

CFPB Director Rohit Chopra stated in October that the "CFPB is suing [the company] for illegally charging hundreds of millions of dollars in enrollment fees through its use of digital dark patterns and online trickery."

This action follows another complaint filed by the CFPB in April of this year against consumer reporting agency TransUnion LLC and John Danaher, a former senior executive, for allegedly continuing to engage in dark patterns that caused consumers seeking free credit scores to unknowingly sign up for a credit monitoring service with recurring monthly charges.

The FTC has been very active in this area too. Recently, it held its annual PrivacyCon, which featured a panel discussion specifically on interfaces and dark patterns.

In September, the FTC issued a report that examined how dark patterns "can obscure, subvert, or impair consumer choice and decision making and may violate the law."

The report highlighted common dark pattern tactics, such as design elements that:

- Induce false beliefs;
- Hide or delay disclosure of material information;
- Lead to unauthorized charges; and
- Obscure or subvert privacy choices.

The report also highlighted a number of enforcement actions the FTC has taken to combat dark patterns. For example, the FTC recently took action against internet phone service provider Vonage Holdings Corp. for allegedly using illegal dark patterns that:

- Forced customers to cancel only by speaking with live agents on the phone, even though customers could sign up for services online, on the phone, and through other methods;

- Made the cancelation process generally difficult;

- Surprised customers with unexpected junk fees when they tried to cancel; and

- Continued to charge customers when they had properly requested that their services be canceled.

This action has resulted in the company paying $100 million in refunds to consumers harmed by the company's actions.

In another action, the FTC alleged credit services company Credit Karma LLC used dark patterns to misrepresent to consumers that they were preapproved for credit cards, but the consumers were usually denied when they applied. As a result, respondents were ordered to pay $3 million.

Most recently, in December, the FTC secured an agreement requiring Epic Games Inc., the creator of popular video game Fortnite, to pay a total of $520 million in relief over allegations the company violated the Children's Online Privacy Protection Act and deployed dark patterns to trick millions of players into making unintentional purchases.

As part of a proposed federal court order filed by the U.S. Department of Justice, the company will pay a $275 million monetary penalty for violating the COPPA Rule.

Under a separate proposed administrative order, it will pay $245 million to refund consumers for its dark patterns and billing practices. This is the FTC's largest refund amount in a gaming case, and its largest administrative order in history.

As to the specific dark patterns allegations, the FTC found the company deployed a variety of dark patterns aimed at getting consumers of all ages to make unintended in-game purchases and then made it difficult for them to cancel or refund those purchases.

Buttons were placed in locations that made it easy for people to tap them without meaning to, while cancel or refund buttons were made difficult to find. In addition, the company did not obtain underage users' parental permission before allowing them to make purchases of in-game currency.

Finally, the FTC alleged the company locked customer accounts completely if they disputed charges with their credit card companies, which meant they lost access to all of their purchases, not just the ones they were disagreeing with.

The company also threatened to lock accounts permanently if users disputed any future charges.

According to the FTC, the company ignored more than 1 million user complaints and numerous employee concerns that many users were being wrongfully charged.

Federal and State Legislators

Federal lawmakers also have acknowledged the potential consumer harm posed by dark patterns and previously introduced the Deceptive Experiences to Online Users Reduction Act, which would have expanded the enforcement power of the FTC to police deceptive acts, including dark patterns.

Although the DETOUR ACT was said to have bipartisan support when introduced at the end of 2021, the bill did not make it past the first stages of the legislative process.

In addition to efforts at the federal level, states have joined the fight through the introduction or passage of privacy legislation that address dark patterns.

California, Colorado, and Connecticut have passed privacy laws that specifically define consumer consent as that which was not obtained through the use of dark patterns, and California further defines dark patterns, as noted above.

The CCPA's proposed regulations devote a full section to consumer consent. Companies may only obtain enforceable consent from consumers if their websites incorporate five principles:

- The use of plain, straightforward language, as opposed to technical or legal jargon;
- Symmetry of choice, where companies may not require consumers to take more steps to opt out of selling personal information than are required to opt in;
- Avoiding elements and language that are confusing;
- Avoiding choice architecture that includes pairing consent to use data for an expected purpose with consent to use data for unrelated purposes; and
- The ease of execution for the consumer in making their choices and decisions.

The proposed regulation also clarifies that if an online interface has the effect of substantially subverting or impairing a user autonomy, decision making, or choice, it will be considered a dark pattern.

The business's intent to design an interface that subverts or impairs user choice, as well as the deliberate ignorance of the interface having that effect, will weigh heavily in favor of finding that a dark pattern exists.

Avoiding Dark Patterns

Dark patterns hurt the consumer experience and create regulatory and legal risks for companies.

The determination that a dark pattern was used in a consumer contract may result in the unenforceability of those agreements, and in monetary and other penalties.

For these reasons, companies should train their legal departments, marketing departments, and web and app interface developers on regulatory guidance and enforcement regarding dark patterns.

These teams should continually flag any dark patterns that are inadvertently being used. In addition, companies should ensure that advertising, website and application flows, and disclosures have the following characteristics:

- Descriptions of the services or products, costs, processes, and other material terms the consumers are agreeing to that contain clear, conspicuous and easy to understand language;
- Clear statements when a company has discretion in the type of product or service offered to avoid the creation or appearance of a bait-and-switch model;
- Fees and other costs that are presented to consumers early on, and specifically not only at the time of checkout;

- Symmetry of choice presented to consumers at the time of decision making, so consumers have equal opportunity to choose any of the available options and that no one option is presented with a design — e.g., highlighting, underlining, flashing, font color or size, or position — that overshadows obscures the rest of the options;

- Ease of cancelation of any memberships or services and properly disclosed consequences of the cancelation; and

- Links to disclosures, selections and opt-outs that are up-to-date and functioning at all times, especially after general updates to the website or app interface.

These steps may help companies be better prepared to address the heightened regulatory scrutiny that seems to be intensifying around dark patterns.

Elizabeth McGinn and Sherry- Maria Safchuk are partners, and Melina Montellanos is an associate, at Buckley LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Elizabeth McGinn, Amanda R. Lawrence, Sherry-Maria Safchuk, David Rivera & Buckley LLP, Shedding Light on Dark Patterns: What Financial Institutions Need to Know, Cybersecurity Law Report, Jul. 21, 2021, at 2-3.