Cybersecurity Law Report
An Acuris company

cslawreport.com

July 21, 2021

FTC ENFORCEMENT

Shedding Light on Dark Patterns: What Financial Institutions Need to Know

By Elizabeth McGinn, Amanda R. Lawrence, Sherry-Maria Safchuk and David Rivera, *Buckley LLP*

Regulators, legislators and private litigants are increasingly looking at how companies attract and conduct business with consumers in online settings, and particularly whether these companies are designing user experiences to manipulate behavior in a way that can prove harmful to the consumer. The inquiry into these so-called "dark patterns" is intensifying, and financial institutions should focus their attention on the potential risks of the online experience they are creating for their customers.

The Federal Trade Commission has pursued enforcement actions involving dark patterns for years, and during a recent public workshop, invited participants to discuss "a range of potentially manipulative user interface designs used on websites and mobile apps." Two members of Congress said at the workshop that they intended to re-introduce legislation in the Senate and House that would empower the FTC to further address the harms arising from them. Several states are also exploring legislation that would target dark patterns.

Class action plaintiffs have already seized upon potential harms from dark patterns to bring claims against companies in multidistrict litigation. State attorneys general also have joined in, relying upon claims that these patterns are unfair, deceptive or abusive acts or practices.

This article will examine the concept of dark patterns, provide common examples of them, analyze regulatory views and actions, and look at what financial institutions should do in light of regulatory focus on dark patterns.

See CSLR's two-part series on the CCPA and online ads: "Facebook Finally Acts, AG Starts Enforcement" (Jul. 29, 2020); "Contract and Compliance Consequences" (Aug. 5, 2020).

The Concept

The term dark pattern has been around for a decade, but academics and industry experts have not yet settled upon one set definition. Most discussions revolve around the concepts of agency, transparency and cognitive biases.

In a September 2020 statement, FTC Commissioner Rohit Chopra defined 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."

Chopra said dark patterns are the "online successor" to direct-mail marketing scams and "pose an even bigger menace:"

Dark pattern tricks involve an online sleight of hand using visual misdirection, confusing language, hidden alternatives or fake urgency to steer people toward or away from certain choices. This could include using buttons with the same style but different language, a checkbox with double negative language, disguised ads, or time pressure designed to dupe users into clicking, subscribing, consenting or buying.

The recent California Privacy Rights Act (CPRA), effective January 1, 2023, with a one-year lookback, defines a 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." The law expressly provides that "agreement[s] obtained through use of dark patterns does not constitute consent." Colorado, Connecticut and Washington introduced privacy rights legislation that each use virtually the same definition of dark pattern as CPRA used.

Broadly speaking, it is helpful to think of a dark pattern as any online user interface designed to lead consumers to an option or choice that benefits the designer when the consumers might not have made that choice if they understood the prompt.

See "Preparing for the CPRA's New Consumer Rights Requirements" (Mar. 10, 2021).

Examples

The FTC's workshop discussed many of the most common types of dark patterns:

- *Dialogues or interfaces that create a "high friction" experience to coerce the consumer.* For example, if a consumer is unable to reject the consent to be tracked dialogue or is required to proceed through several screens to deny consent, then these dialogues can increase the likelihood that a consumer will signal consent without intending to do so. These pop-up dialogues are a gateway for a company to increase its market power by gaining valuable personal information about the consumer and micro-target them with tailored advertising designed to steer the consumer away from competitors.
- *Websites that make it difficult to cancel subscriptions.* During the FTC workshop, Representative Lisa Blunt Rochester recounted her experience with a $39 per month birdwatching application that made it difficult to opt out of or cancel the subscription.
- *Eliminating certain options from the website interface.* Consumers may encounter this type of pattern when they "consent" to multiple agreements with one checkbox.
- *Certain auto-replay features directed at vulnerable consumers.* This type of dark pattern may include auto-replay features that expose minors to inappropriate videos.

- *Acting on a user's bias to persuade the consumer to do something*. This may involve informing the consumer that others are also viewing the same items or that there are a limited number of items that may be purchased.
- *Limiting disclosure of essential information until the user is substantially invested in the activity*. One example is a fee that often is not disclosed until late in the purchasing process. This type of dark pattern may arise if a consumer is unable to proceed to certain websites without payment. A consumer advocacy group observed that over 6,000 consumers had complained to the FTC in 2018 about lack of fee transparency in online ticketing services. One paper studied several million online ticket shoppers who were not presented with upfront fees. Those users ended up spending 20 percent more than the control group and were 14 percent more likely to complete the transaction on the platform that employed the dark pattern.
- "*Confirmshaming*," *where charged language steers a user to a particular choice*. This type of dark pattern intends to shame the consumer into a particular choice that benefits the designer (*e.g.*, signing up to receive emails of special offers instead of clicking "No thanks, I don't want to save money.").
- *Using confusing language or visual interference* (*e.g.*, opt-out boxes that are greyed so as to seem unavailable).

Artificial intelligence can also create personally tailored dark patterns that provide a different online navigational experience for each user. One panelist described a commercial targeting engine that uses over 70 personal data variables to show specific segments of visitors' particular website content.

Companies now have the tools to customize their websites in almost unlimited ways depending on the consumer. New technologies, like A/B testing, allow marketers to quickly and cheaply test, refine and personalize user interfaces to maximize click-throughs, consents and purchases. This adaptability drives sales and data collection.

See CSLR's AI Compliance Playbook series: "Traditional Risk Controls for Cutting-Edge Algorithms" (Apr. 14, 2021); "Seven Questions to Ask Before Regulators or Reporters Do" (Apr. 21, 2021); and "Understanding Algorithm Audits" (Apr. 28, 2021).

Regulators' View

The FTC has been pursuing dark patterns for years. Daniel Kaufman, the acting director of FTC's Bureau of Consumer Protection, said the Commission would work with states and other international partners to investigate dark patterns, warning that companies should "expect … continued aggressive FTC enforcement in this area." He also observed a number of the panelists had argued for "additional rules, policy statements or enforcement guidance" surrounding dark patterns, and said the FTC is "carefully considering all options and nothing is off the table."

The FTC already yields statutory authority to pursue dark pattern abuses. For example, Sections 5 and 18 of the FTC Act grant it the

power to combat unfair or deceptive acts or practices. The Restore Online Shoppers' Confidence Act and the CAN-SPAM Act also allow the FTC to pursue persons that use unclear website disclosures or deceptive email headers, or do not offer consumers simple opt-out features.

The FTC brought dark pattern enforcement actions against businesses when there was even less of a public mandate. The FTC workshop cited one case where the Ninth Circuit reviewed the boilerplate language in the terms and conditions and found that, although the document was "technically correct," the entity would still be held liable under Section 5.

Chopra, who awaits confirmation as the director of the CFPB, made clear his interest in dark patterns in his September 2020 statement. He denounced a company's practice of making its subscription fees difficult to cancel, citing "a maze of 'privacy' settings so complex that their own engineers and employees can't crack the code." He also argued that for the FTC to be a "credible watchdog," it must "methodically use all of [its] tools" to counter "popular, profitable, and problematic" dark pattern business practices. Chopra's remarks may be a preview of how the CFPB will approach dark pattern enforcement.

State regulators are also bringing cases that implicate dark patterns. For example, the Office of the Attorney General for the District of Columbia has an action pending against a food delivery company for allegedly adding a 10-percent default charge to customer's bills through a dark pattern. That default charge was presented as a tip for the deliverer, and the consumer could increase, decrease or waive that amount. However, the fee went to the company and not to workers.

See CSLR's two-part series on takeaways from former FTC officials on the Commission's 2019 enforcement: "General, Financial and Children's Privacy" (Apr. 8, 2020); and "Data Security Guidance and Enforcement Predictions" (Apr. 15, 2020).

Class Actions

Consumers are also becoming aware of the use of dark patterns, and plaintiffs' counsel are bringing claims against companies for their alleged use. In a recent class action filed against a media sharing platform, plaintiffs alleged that the platform "used 'dark patterns' in [its] user interfaces to trick users into doing things they might not otherwise do, like signing up for recurring bills" and maintaining subscriptions through complex cancellation procedures. Several similar lawsuits have been filed against companies in the past couple of years, all alleging the use of deceptive dark patterns that manipulate users to engage in certain behaviors to the detriment of the consumer (see, *e.g.*, *Nichols v. Noom, Inc.*; *Sherman v. Facebook, Inc.*; *Farmer v. Airbnb, Inc.*; *Rattner v. Tribe App, Inc.*).

Legislative Efforts

Representative Rochester and Senator Mark Warner said they will re-introduce the Deceptive Experiences To Online Users Reduction Act (DETOUR Act), which will prohibit major social media platforms from using deceptive user interfaces. The DETOUR Act as introduced in 2019 would have made it unlawful for, in relevant part, "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."

Considerations for Financial Institutions

FTC and legislative attention to dark patterns should compel companies to consider reexamining the design architecture of their websites and computer applications – especially financial institutions that may face allegations from federal and state regulators that such patterns are unfair, deceptive or abusive acts or practices. The present lack of precision about which design interfaces could invite investigation is a complication for financial institutions and related entities looking to mitigate enforcement risk, but such entities, by way of their legal, compliance, and marketing/business departments, may consider:

- *Preparing now to respond to consumer and regulator questions regarding the use of dark patterns*. The prevailing opinion of panelists at the FTC's workshop suggests that dark patterns are everywhere, and consumers will begin to have questions about whether a company is using dark patterns. Entities should review past FTC guidance and applicable federal and state case law to determine what questions consumers may ask.
- *Identifying how they currently obtain online consumer consent to enter into agreements, and to collect personal information*. Reviewing all consumer-facing webpages and prompts will help companies determine whether there are areas where consumers may be experiencing dark patterns and whether further enhancements to its webpages and prompts are warranted. For instance, an expensive add-on at check-out that is pre-selected may invite customer complaints and regulatory questions. In the end, regulators must be assured that consumers are able to comfortably make informed decisions about the information companies collect.
- *Assessing whether their webpages and prompts give rise to dark patterns that disproportionally affect vulnerable individuals and communities*. For instance, research indicates that apps employ dark patterns more frequently than either a mobile browser or a desktop website. Not all internet users own multiple devices, and certain "vulnerable individuals" are more likely to use apps to access entities, which may raise social equity concerns.

Increased regulation of dark patterns is imminent. Federal and state regulators are paying more attention to their use, and consumers are asking questions about how to avoid them. Financial institutions and related entities will need a united strategy for responding to questions about dark patterns from regulators and consumers.
They should take action now to limit the risks that may arise from their heightened interest.

Elizabeth E. McGinn, a partner at Buckley LLP, focuses her practice on assisting clients in identifying, evaluating and managing the risks associated with cybersecurity, internal privacy and information security practices, as well as those of third-party vendors. A significant part of her practice involves addressing data security breaches, working proactively with clients to prevent data security breaches and responding to regulatory inquiries, investigations and enforcement actions related to privacy, information security and cybersecurity issues.

Amanda R. Lawrence is a partner at Buckley LLP, where she assists clients in managing cybersecurity, privacy, information security and vendor risks and compliance, as well as evaluating and addressing potential data security incidents, including drafting consumer and regulator notifications. She has a focus on financial services industry issues, including privacy, cybersecurity, data breach, class actions and FTC and other regulator priorities.

Sherry-Maria Safchuk is counsel in the Los Angeles office of Buckley LLP, and assists clients on privacy issues, including those related to the CCPA. She represents clients in regulatory and compliance matters and provides support for complex litigation and government investigations involving the mortgage, consumer and commercial lending industries.

David Rivera is a litigation attorney at Buckley LLP. His practice includes assisting clients with privacy, data security and information governance issues, as well as state breach notification laws.