LOOKING BEYOND THE PRIVACY POLICY: REGULATORY SCRUTINY OF DARK PATTERNS IN USER INTERFACES

BY CHRISTINE CHONG

& CHRISTINE LYON

Freshfields Bruckhaus Deringer U.S. LLP.

TechREG CHRONICLE
MAY 2023

Visit www.competitionpolicyinternational.com for access to these articles and more!

LOOKING BEYOND THE PRIVACY POLICY: REGULATORY SCRUTINY OF DARK PATTERNS IN USER INTERFACES

By Christine Chong & Christine Lyon

Privacy regulators are increasingly looking beyond a company's privacy policy to scrutinize the user interface of its websites, apps, and other online services, and challenging designs that they view as manipulating consumer choice. In this pursuit, regulators and privacy advocates increasingly utilize the term "dark patterns" as an umbrella concept to describe the wide array of activities that may be considered manipulative design in user interfaces. The "dark patterns" concept also provides a tool for regulators and legislators to challenge practices that they believe undermine meaningful consumer choice. In this article, we examine the developing dark pattern regulatory enforcement landscape from a data privacy perspective, with a focus on recent U.S. and EU regulatory developments.

01

WHAT IS MEANT BY "DARK PATTERNS" IN THE PRIVACY CONTEXT?

The term "dark patterns" was reportedly coined in 2010 by Harry Brignull, a user interface designer, and the term has since been increasingly and formally adopted by privacy advocates and regulators.[2] In his original piece, Brignull suggested that deceptive user interfaces are common on the web because dark patterns may be subtle and unnoticeable: "in isolation they're usually so small that each one is barely annoying enough for people to do anything about them."[3] While dark patterns may be just "barely annoying" for an individual user, he noted that dark patterns tend to perform well for businesses, and that these subtle interface designs tended to escape legal scrutiny. Over time, he observed that many businesses implemented dark patterns "by mistake or misadventure," and that they often viewed these changes as "improvements" to interfaces.[4]

Dark patterns are no longer bypassing legal challenge and over recent years, the FTC has regularly invoked the concept of "dark patterns" in the context of Section 5 of the FTC Act for unfair or deceptive practices. This past fall, the FTC issued a staff report on dark patterns, Bringing Dark Patterns to Light.[5] The FTC uses the term "dark patterns" to describe a range of design practices on website and mobile app interfaces that trick or manipulate users into making choices they would not otherwise make and that may cause harm.[6] The FTC views these dark patterns as concerning because they may impair consumer choice, whether intentionally or unintentionally.[7] The FTC observes that dark patterns are frequently used in combination, giving the dark patterns a stronger effect than if a single dark pattern was used alone. Further, the FTC notes that dark patterns are not limited to certain industries and contexts, but can be found on children's apps, cookie consent banners, and ecommerce sites.[8] Dark patterns raise particular concerns in the enforcement context because, by nature, dark patterns are discreetly implemented and may not be obvious to the average user. For example, the FTC's staff report flags various examples of privacy-related practices that may constitute dark patterns, by obscuring or subverting privacy choices:

- Interfaces that repeatedly prompt users to select settings they have already declined;
- Interfaces that present confusing toggle settings that lead users to make unintended privacy choices;
- Interfaces that purposely obscure privacy choices and make the privacy choices difficult to view (such as placing links to privacy disclosures in a font size or color that makes them difficult to see) or otherwise access (such as settings "buried in a privacy policy");
- Interfaces that highlight a choice that allows for more data collection, while minimizing and greying out another option that would enable users to limit the data collection; and
- Interfaces that include default settings that maximize data collection and sharing.[9]

Although the FTC has refrained from providing bright-line standards for determining when user interface design features will be considered "dark patterns," the FTC's staff report and enforcement actions provide useful guidance. The FTC's enforcement activities further reflect the FTC's close attention to the following types of privacy-related practices:

- **Notice of privacy settings**. For example, in an enforcement action involving smart televisions, the FTC asserted that the manufacturer failed to provide notice of a default setting which allowed it to collect and share certain data regarding a user's television viewing activity with third parties.[10] Even where the manufacturer began to provide initial

2 Harry Brignull, *Dark Patterns: Deception vs. Honesty in UI Design,* A LIST APART (Nov. 1, 2011), https://alistapart.com/article/dark-patterns-deception-vs.-honesty-in-ui-design/.

3 *Ibid.*

4 *Ibid.*

5 FTC Staff Report, *Bringing Dark Patterns to Light*, FTC.GOV, (Sep., 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

6 *Ibid.* at 2.

7 *Ibid.*

8 *Ibid.* at 3.

9 *Ibid.* at 18.

10 *Ibid.* at 17.

pop-up notices, the FTC alleged that the notices would time out and only be shown to users for 30 seconds, which the FTC did not view as sufficient notice.[11]

· **Ease of access to privacy settings**. In the same action, the FTC asserted that the initial pop-up notice did not link to a settings menu or privacy policy enabling the user to change the setting related to disclosure of television viewing activity. Even where users reached the settings menu, the FTC alleged that the relevant setting did not expressly address the collection of viewing data, and therefore did not offer consumers meaningful and informed choice.[12]

· **Transparency and clarity of privacy-related disclosures.** In another action, the FTC alleged that a health app made deceptively broad privacy assurances in large, high-contrast, "unavoidable" text in its user interface, in order to encourage users to complete a health questionnaire, while placing the links to the privacy policy (which provided lesser assurances) in small, low contrast, "barely visible" text.[13] The FTC alleged that the privacy assurances in the user interface were misleading and constituted dark patterns that effectively dissuaded users from reading the privacy policy.

Following its September 2022 staff report, the FTC also issued a press release announcing its intention to increase enforcement against practices that the FTC views as dark patterns.[14]

02

DARK PATTERNS IN U.S. STATE CONSUMER PRIVACY LAWS

The concept of "dark patterns" has now made its way into statutory law as well, in several of the new comprehensive state consumer data privacy laws. The California Consumer Privacy Act ("CCPA"),[15] Connecticut Data Privacy Act ("CTDPA"),[16] and Colorado Privacy Act ("CPA")[17] each generally define "dark patterns" as "a user interface designed or manipulated with the ***substantial effect of subverting or impairing user autonomy, decisionmaking, or choice***" (emphasis added)[18] and provide that consent obtained through the use of dark patterns is not valid.[19]

Notably, accompanying rules and regulations to the CCPA and CPA further raise the bar for businesses by stating that certain potential defenses that businesses may raise about dark patterns would not be appropriate. The CCPA regulations clarify that whether the businesses had "intent" for an interface to be a dark pattern does not determine whether the user interface actually is a dark pattern, but that intent is merely a factor to be considered.[20] Additionally, the CCPA regulations state that if the business knows of, but does not remedy, a user interface that subverts or impairs user choice, the user interface may still be considered a dark pattern.[21] The CPA rules add that the fact that a design or practice is commonly used is not by

11 FTC Complaint, *FTC v. Vizio, Inc. and Vizio Inscape Servs., LLC*, Case No 2:17-cv-00758 (D. N.J.), 6-7, https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.

12 *Ibid.*

13 FTC Complaint, *In the Matter of BetterHelp*, FTC Matter No. 2023169, paras. 33-34, https://www.ftc.gov/system/files/ftc_gov/pdf/2023169-betterhelp-complaint_.pdf.

14 FTC, *FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions*, FTC.GOV (Oct. 28, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions.

15 *California Privacy Rights Act of 2020*, Cal. Civ. Code § 1798.100 (2020).

16 *Connecticut Data Privacy Act*, Conn. Gen. Stat. Ann. §§ 42-515 to 42-525.

17 *Colorado Privacy Act,* Colo. Rev. Stat. Ann. §§ 6-1-1301 to 6-1-1313.

18 Cal. Civ. Code 1798.140(l); Conn. Gen. Stat. Ann. §§ 42-515(11); Colo. Rev. Stat. Ann. § 6-1-1303(9).

19 Cal. Civ. Code 1798.140(h); Conn. Gen. Stat. Ann. §§ 42-515(6)(C); Colo. Rev. Stat. Ann. § 6-1-1303(5)(c). Notably, these laws require consent only in certain limited circumstances, but they do impose heightened standards for consent when it is required.

20 11 CCR § 7004(c).

21 *Ibid.*

itself a sufficient defense that a design or practice is not a dark pattern.[22]

These state consumer data privacy laws take the concept of "dark patterns" beyond the realm of regulators and advocates into statutory law. With more states working on similar laws of their own, companies can expect greater express regulation of "dark patterns," in addition to the use of this concept in FTC and other consumer protection enforcement actions.

03
DARK PATTERNS REGULATORY ACTIVITY IN THE EU

Outside of the U.S., the European Union is ramping up its interest and activities surrounding dark patterns as well. In January 2023, the EU Commission and national consumer protection authorities conducted a sweep of retail websites to assess how frequently dark patterns are used. The sweep resulted in a finding that 40 percent (148 out of 399) of online retailers used at least one of the following three dark patterns: fake countdown timers with deadlines to purchase specific products, web interfaces designed to lead consumers to purchases or other choices through visual design or choice of language, and hidden or less visible information.[23] Following this sweep, these businesses were contacted to correct their retail websites and the EU Commission released a statement calling on national authorities to use their enforcement and binding tools to tackle these dark patterns issues.

There is also guidance from international data protection authorities, such as the guidance from the European Data Protection Board ("EDPB") on dark patterns.[24] The EDPB guidelines provide detailed guidance specifically for social media platforms about how to assess and avoid dark patterns in social media user interfaces that violate EU General Data Protection Regulation ("GDPR") principles. Although the EDPB guidelines are directed to social media platforms, the principles are relevant to other types of websites and online services as well. The EDPB's guidelines refrain from stating definitive or bright-line standards for determining whether a user interface design involves dark patterns, but caution about the following categories of dark patterns:

- **Overloading**: Prompting the user with a large number of requests, information, options, or possibilities, thus pushing users to share more data. The EDPB explains that users tend to experience decision-fatigue from having to refuse the request each time they visit an online service and are therefore likely to end up giving in to submit data in order to make the prompts go away. For example, the EDPB indicates that overloading may occur when a social media provider repeatedly asks for a phone number every time a user logs onto an account, even though the user has previously refused to provide the phone number during the sign-up process or last login.
- **Skipping:** Creating a distraction to make users forget or not fully consider the data they are going to share through the interface. In particular, if data settings are preselected or not able to be changed on a first layer, this may nudge individuals to keep the default preselected option.
- **Stirring:** Using patterns, wording, or visuals to positively or negatively 'emotionally steer' users. The examples provided by the EDPB guidelines suggest that even subtle emotional steering (such as urging users not to be a "lone wolf" and instead to share their geolocation data with others to "make the world a better place") may be considered a dark pattern.
- **Hindering:** Obstructing or blocking users from making informed decisions about their data. The EDPB suggests that this can include displaying a pop-up window asking, "Are you sure?" if the user clicks the "skip" button to try to avoid entering certain types of data, or otherwise prolonging the sign-up process if the user selects more privacy-protective choices. The EDPB also gives an example of failing to provide a ready means for individuals to withdraw consents they may have provided previously.
- **Left in the dark:** Ambiguous wording or information leaving users unsure of how their data will be processed.

Although the EDPB guidelines are based on EU General Data Protection Act ("GDPR") principles, they share many

22 4 CCR 904-3, Rule 7.09(B).

23 Press Release, European Commission, Consumer protection: manipulative online practices found on 148 out of 399 online shops screened, (Jan., 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418.

24 EDPB, *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*, (March 14, 2022), EDPB, https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf.

similar concepts with the FTC's view of dark patterns as described above.

04
LOOKING AHEAD

The evolution of the "dark patterns" concept from UX designers to regulators and now legislators reflects how the U.S. is moving toward more formal regulation and oversight of consumer data practices online. It is interesting to see that U.S. and EU regulators are raising similar concerns about dark patterns in the context of consumer digital activity online, notwithstanding the significant differences between U.S. and EU data privacy regimes. Regulators are looking beyond the text of a company's formal privacy policy or privacy notice to assess the user experience holistically, and are more inclined to delve into technical details of how information and choices are presented to consumers. These developments underscore the importance of businesses assessing the privacy impacts of their user interfaces to avoid practices that may be considered dark patterns.

> *Outside of the U.S., the European Union is ramping up its interest and activities surrounding dark patterns as well*

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY® INTERNATIONAL