DRAWING LINES AROUND DARK PATTERNS

BY MANEESHA MITHAL

& STACY OKORO

Maneesha Mithal is a partner at the law firm of Wilson Sonsini Goodrich & Rosati. Stacy Okoro is an associate at Wilson Sonsini Goodrich & Rosati.

TechREG CHRONICLE
MAY 2023

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

DRAWING LINES AROUND DARK PATTERNS

By Maneesha Mithal & Stacy Okoro

The practice of nudging consumers toward particular choices is nothing new. We have all experienced the allure of picking up a sweet treat along the checkout lane as we wait to pay for our groceries. But regulators have been increasingly focused on combating so-called dark patterns online that may substantially influence or interfere with consumer decision-making. This article chronicles the origins of the phrase "dark patterns," discusses the current US regulatory landscape on dark patterns, and sets forth theories as to why this issue has become such a focus for regulators over the past several years. It concludes with some tips for companies on how to avoid regulatory scrutiny relating to dark patterns.

01

WHAT'S THE DEAL WITH DARK PATTERNS?

The practice of nudging consumers toward a particular choice is nothing new. We have all experienced the allure of picking up a sweet treat along the checkout lane as we wait to pay for our groceries. But regulators have been increasingly focused on combating so-called dark patterns online that may substantially influence or interfere with consumer decision-making. The term "dark patterns" was originally coined by a UX/UI designer named Harry Brignull in 2010 to describe "tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something."[2] Researchers have traced the dark patterns we experience today as a result of decades-long trends in the organizational psychology techniques in brick-and-mortar stores, the study of behavioral economics and heuristics to understand consumer decision-making, and the emergence of business growth strategies using user interface design techniques.[3]

There is still no universal definition of what constitutes a dark pattern, despite years of research since Brignull originally coined the term. But regulators generally refer to dark patterns as the practices or formats that can manipulate or mislead consumers into taking actions that would not otherwise reflect their true preferences, intent, or consent. Some researchers and regulators believe that dark patterns are particularly concerning in the digital privacy context because they go further than previous manipulation in the offline world by using intrusive privacy settings to create personalized interfaces that take advantage of user psychology, biases, or emotions.[4]

Over the past several years, regulators have increasingly focused their attention on combating dark patterns. In 2018, the Norwegian Consumer Council, a consumer protection authority, published a report called "Deceived by Design."[5] The report defined dark patterns in the privacy context as "techniques and features of interface design meant to manipulate users [and] to nudge [them] towards privacy intrusive options[, including] privacy intrusive default settings, misleading wording, giving users an illusion of control, hiding away privacy-friendly choices, take-it-or-leave-it choices, and choice architectures where choosing the privacy friendly option requires more effort for the users."[6] In the consumer protection context, in 2020, the Federal Trade Commission ("FTC") brought a case against an online education company that allegedly misrepresented their subscription cancellation practices.[7] In his concurring statement, then-Commissioner Rohit Chopra described concerns about the types of dark patterns he believed to be evident in that case 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."[8] With increasing regulatory interest, the stage was set for further legislative, rulemaking, and enforcement efforts to combat dark patterns.

02

CURRENT U.S. REGULATORY LANDSCAPE ON DARK PATTERNS

Regulators in the U.S. and the EU have been active in addressing dark patterns either by using the term in connec-

2 Harry Brignull, What are deceptive patterns?, Deceptive Design, https://www.deceptive.design/index.html.

3 Arvind Narayanan, Arunesh Mathur, Marshini Chetty & Mihir Kshirsagar, Dark Patterns: Past, Present, and Future, 18 ACM Queue 67 (2020).

4 See e.g. Fed. Trade Comm'n, Bringing Dark Patterns to Light, STAFF REPORT 3 (September 15, 2022); Ryan Calo, Digital Market Manipulation, 82 Geo. Wash. L. Rev. 995, 1021 (2014); Justin Hurwitz, Designing a Pattern, Darkly, 22 N.C. J.L. & Tech. 57, 67–68 (2020) (suggesting that what is unique about dark patterns is that, in the online context, "[t]here is practically no limit to design choices, and those design choices can be changed, tweaked, updated, and targeted with ease").

5 Norwegian Consumer Council, Deceived by Design, FORBRUKER RADET 13–18 (June 27, 2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

6 *Id.* at 3.

7 *FTC v. Age of Learning, Inc.*, Case No. 2:20-cv-7996 (C.D. Cal.).

8 Prepared Remarks of Commissioner Rohit Chopra Regarding Dark Patterns in the Matter of Age of Learning, Inc. Commission File Number 1723186 (Sept. 2, 2020), https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf.

tion with existing laws, engaging in new rulemakings, or offering guidance. Some examples follow.

A. State Privacy Laws

The California Privacy Rights Act ("CPRA"), which amended the California Consumer Privacy Act ("CCPA") and came into effect on January 1, 2023, defines dark patterns 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."[9] The CPRA uses the term to limit the types of design patterns that can constitute "consent" under the law, noting that any "agreement obtained through the use of dark patterns does not constitute consent,"[10] and empowers the California Privacy Protection Agency ("CPPA") to promulgate rules regarding dark patterns.[11] The CPPA filed a rulemaking package containing these rules with California's Office of Administrative Law for review on February 14, 2023. The proposed rules generally require that privacy choices be easy to understand and execute, be symmetrical, avoid confusing language or interactive elements, and avoid choice architecture that impairs or interferes with the consumer's ability to make a choice. They include a number of more specific examples. For example, they state that "Yes" and "Ask me later" are not symmetrical choices; nor are "Accept All" and "Preferences." Rather, the regulations suggest that the symmetry requirement would be met by "Yes" and "No" or "Accept All" and "Decline All." Also notable, the proposed rules state that a business's design intent is not determinative in whether an interface is a dark pattern, but is a factor to be considered. Thus, user interfaces may be considered a dark pattern under CPRA even where a business did not intend to subvert or impair user choice.

In a similar vein, the Colorado Privacy Act ("ColoPA"), which comes into effect on July 1, 2023, adopts an identical definition of "dark pattern"[12] and states that consent obtained through dark patterns is invalid.[13] The Colorado attorney general released a set of proposed regulations that define with more specificity what constitutes a dark pattern. In some respects, the Colorado regulations go further than the California regulations. For example, they explicitly prohibit pre-checked boxes, state that silence or failure to take affirmative action should not be interpreted as consent, and contain specific prohibitions against using "emotionally manipulative language or visuals."[14] But the Colorado regulations appear narrower in at least two respects. First, the proposed regulations make clear that the principles set forth in the regulation constitute "factors" in determining a dark pattern, as opposed to individual requirements. And second, unlike the California regulations, which prohibit dark patterns when designing data subject access request interfaces as well as consent interfaces, the Colorado proposal would prohibit dark patterns only on user interfaces used to obtain consent required under the statute.[15]

Finally, Connecticut's new privacy law, "An Act Concerning Personal Data Privacy and Online Monitoring," comes into effect in July 2023 and similarly adopts the same definition of dark pattern and invalidates consent obtained through dark patterns. Notably, although it does not call for regulations to define dark patterns with more specificity, as the CPRA and ColoPA do, the Connecticut law defines dark patterns as including "any practice the Federal Trade Commission refers to as a 'dark pattern.'"[16]

> ***"Connecticut's new privacy law, "An Act Concerning Personal Data Privacy and Online Monitoring," comes into effect in July 2023 and similarly adopts the same definition of dark pattern and invalidates consent obtained through dark patterns***

9 Cal. Civ. Code § 1798.140(l). California also passed the Age Appropriate Design Code Act in August 2022, and there is a provision to also regulate the use of dark patterns as they apply to online services likely to be accessed by children under the age of 18.

10 Cal. Civ. Code § 1798.140(h).

11 Cal. Civ. Code § 1798.185(20)(C)(iii).

12 Colo. Rev. Stat. § 6-1-1303(9).

13 Colorado Privacy Act, Senate Bill 21-190, § 6-1-1303(5)(c), available at https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf.

14 Colorado Privacy Act, Version 3 of Proposed Draft Rules, Rule 7.09(A), available at https://coag.gov/app/uploads/2023/01/CPA_Version-3-Proposed-Draft-Regulations-1.27.2023.pdf.

15 Colorado Privacy Act, Version 3 of Proposed Draft Rules, available at https://coag.gov/app/uploads/2023/01/CPA_Version-3-Proposed-Draft-Regulations-1.27.2023.pdf.

16 Section 1(11), Public Act No. 22-15: https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF.

B. FTC Guidance and Enforcement Actions

Although the phrase "dark patterns" has only recently entered the regulatory lexicon, the FTC's entire deceptive advertising enforcement program over the past century can be characterized as combating dark patterns. Well before online advertising became ubiquitous, the FTC challenged fine-print disclosures in print ads. See e.g. *FTC v. Häagen-Dazs Co*., 119 F.T.C. 762 (1995) (consent order) (challenging effectiveness of fine-print footnote modifying claim that frozen yogurt was "98% fat free"); *FTC v. Stouffer Food Corp*., 118 F.T.C. 746 (1994) (holding that sodium content claims for Lean Cuisine products were false and unsubstantiated and not cured by fine-print footnote). The FTC applied these same principles to Internet advertising, challenging material disclosures made in hyperlinks and mouseover text.[17] The FTC issued its deceptive advertising guidance known as the "Dot Com Disclosures" in 2000,[18] and updated that Guidance in 2013 to provide information to companies on how to ensure effective online disclosures.[19] The guidance focused on whether qualifying information would be considered clear and conspicuous, by focusing on four factors:

- Prominence: whether the qualifying information is prominent enough for consumers to notice and read (or hear)
- Presentation: whether the qualifying information is presented in easy-to-understand language that does not contradict other things said in the ad and is presented at a time when consumers' attention is not distracted elsewhere
- Placement: whether the qualifying information is located in a place and conveyed in a format that consumers will read (or hear)
- Proximity: whether the qualifying information is located in close proximity to the claim being qualified.

Against this backdrop, in September 2022, the FTC released a new guidance document entitled "Bringing Dark Patterns to Light."[20] In many ways, this guidance repeats some of the principles the FTC has been discussing since 2000: It advises advertisers to, for example, refrain from making false claims; disclose material information about endorsers' relationship to advertisers; and make clear the nature of any subscription schemes. But the report seems to call out other practices in ways that are less clear. For example, it cites as a potential dark pattern "parasocial relationship pressure," such as using cartoon characters to encourage in-app purchases; use of virtual currencies; and practices such as nagging or shaming. The report, while focused on consumer protection issues generally, frequently cites problems associated with dark patterns in the privacy space, such as asymmetrical choices to accept or reject data collection.[21]

Against this backdrop, in September 2022, the FTC released a new guidance document entitled "Bringing Dark Patterns to Light

After the release of the report, in announcing several consumer protection enforcement actions, the FTC used the term "dark patterns" to describe alleged misconduct, when in reality the alleged conduct generally ran afoul of a traditional application of the FTC's Section 5 deception authority. For example, in November 2022, the FTC alleged Vonage used dark patterns to make it difficult for consumers to cancel their service over the phone, to impose early termination fees on customers who requested cancellation despite the fees not being clearly disclosed at sign-up, and to charge consumers even after they requested cancellation, in violation of the Restore Online Shoppers Confidence Act, 15 U.S.C. §§ 8401-8405 (ROSCA).[22]

The FTC also announced several proposed rules with the stated purpose of combating dark patterns. For example, in its Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security, the FTC stated that, "[t]he Commission's enforcement actions have targeted several

17 *In the Matter of Michael D. Miller, individually and d/b/a Natural Heritage Enterprises*. FTC Matter No. 9923225

18 Fed. Trade Comm'n, *Dot Com Disclosures: Information about Online Advertising* (May 3, 2000), available at https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-issues-guidelines-internet-advertising/0005dotcomstaffreport.pdf.

19 Fed. Trade Comm'n, *.com Disclosures: How to Make Effective Disclosures in Digital Advertising* (March 12, 2013), available at https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf.

20 Federal Trade Commission, Bringing Dark Patterns to Light, STAFF REPORT 3 (September 15, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

21 Federal Trade Commission, Bringing Dark Patterns to Light, STAFF REPORT 3 (September 15, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

22 Press Release, Fed. Trade Comm'n, FTC Action Against Vonage Results in $100 Million to Customers Trapped by Illegal Dark Patterns and Junk Fees When Trying to Cancel Service (November 3, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/11/ftc-action-against-vonage-results-100-million-customers-trapped-illegal-dark-patterns-junk-fees-when-trying-cancel-service.

pernicious dark pattern practices, including burying privacy settings behind multiple layers of the user interface."[23] Similarly, in a press release announcing its proposed rulemaking on junk fees, the FTC stated that "Companies often harvest junk fees by imposing them on captive consumers or by deploying digital dark patterns and other tricks to hide or mask them."[24]

C. Other Developments

Increased scrutiny of dark patterns is not limited to U.S. regulators. European consumer protection and privacy regulators have also increased their focus on dark patterns. In December 2021, the European Commission published guidance to clarify that the Unfair Commercial Practices Directive ("UCPD") applies to dark patterns.[25] Likewise, in March 2022, the European Data Protection Board ("EDPB") released a report titled "Dark patterns in social media platform interfaces: How to recognise and avoid them."[26] And earlier this year, European consumer protection authorities announced a sweep of 399 retail websites and found so-called dark patterns present on 148 of them.[27]

Self-regulatory organizations have also provided guidance on dark patterns. In April 2022, the Network Advertising Initiative ("NAI"), a self-regulatory association of ad-tech companies, issued a report to help its member companies understand dark patterns.[28] The NAI outlined several general best practices mostly derived from law, regulations, and guidance on dark patterns from the U.S. and EU, and also offered a number of recommendations for both crafting notice-and-consent prompts and designing user interfaces.

Finally, members of Congress have been interested in developing dark patterns legislation. For example, in November 2021, representatives from Delaware and Ohio introduced the Deceptive Experiences to Online Users Reduction ("DETOUR") Act.[29] So far, the bill has not been reintroduced in the 118th Congress.

03
OBSERVATIONS, CONSIDERATIONS, AND ANALYSIS

Dark patterns have become a major regulatory focus in the past couple of years, but why? Why is the issue becoming so ubiquitous now? What forces are at play? This section attempts to provide some answers to these questions by analyzing some of the reasons regulators may be so focused on dark patterns:

- **Concerns about aggressive marketing tactics:** For years, regulators have focused on aggressive marketing tactics that often target vulnerable consumers. These practices include investment scams, work-at-home opportunities, credit repair schemes, dietary supplements that make unsubstantiated health claims, and many others. Regulators understandably want to put up strong and clear guard rails to curb these ubiquitous and harmful practices.
- **Skepticism about the ability of consumers to exercise meaningful choices:** In the privacy context in particular, there have been numerous articles, reports, studies, workshops, and opinion pieces analyzing the difficulty consumers have in understanding how their data is collected, used, and shared, let alone make meaningful choices about that conduct. For many

23 Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 512273, 51275 at https://www.federalregister.gov/d/2022-17752.

24 Press Release, Fed. Trade Comm'n, Federal Trade Commission Explores Rule Cracking Down on Junk Fees (October 20, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/10/federal-trade-commission-explores-rule-cracking-down-junk-fees.

25 European Comm'n, Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, EUROPEAN COMMISSION (December 21, 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1229(05)&from=EN (although CPRA and CPA regulations and the FTC's guidance have considered the effect of dark patterns on vulnerable populations, the UCPD would explicitly find a dark pattern used to exert undue influence over a vulnerable population, in certain circumstances, a violation of the Directive).

26 European Data Protection Board, Guideline 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them, EDPB (March 21, 2022), https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en.

27 Press Release, European Comm'n, Consumer protection: manipulative online practices found on 148 out of 399 online shops screened (January 30, 2023): https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418.

28 National Advertising Initiative, Best Practices for User Choice and Transparency, NAI (May 10, 2022), https://thenai.org/best-practices-for-user-choice-and-transparency/.

29 H.R.6083 - 117th Congress (2021-2022): Deceptive Experiences To Online Users Reduction Act, H.R.6083, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/house-bill/6083.

years, the regulatory focus had been on how to provide consumers with the necessary information to make informed choices, such as through "just-in-time disclosures," and standardized formats (e.g. nutrition labels). The debate also involved whether companies should provide consumers with choices on an opt in or opt out basis. Now, concerns have been expressed that, even with opt-in frameworks, such as the EU cookie directive and Apple's app tracking transparency framework, consumers are becoming numb to such disclosures, and are deterred from exercising meaningful choices.[30] And the FTC has brought numerous cases involving companies allegedly obscuring privacy choices.[31] The FTC and state privacy regulators are likely focused on dark patterns in privacy choice architecture because of these concerns.

- **Concerns about court decisions:** The FTC suffered a loss in 2021 at the Supreme Court in *AMG Capital Management LLC v. FTC*, where the Court ruled that the agency could not seek consumer redress in federal district court under Section 13(b) of the FTC Act.[32] From the late 1970s to 2021, federal courts had read this provision to allow the FTC to obtain consumer redress as an equitable remedy for violations of the FTC Act, but the Supreme Court curtailed that option. As a result, the FTC has been searching for alternative ways to get monetary relief and impose monetary penalties. One way the agency can do so is by issuing rules that describe with specificity what constitutes unfair or deceptive acts or practices. As noted above, the FTC has initiated several rulemaking proceedings under the guise of combating dark patterns. Creating more bright-line rules around dark patterns would enable the FTC to get monetary fines from companies that violate those rules.
- **Concerns about competition:** In addition to protecting consumers from deceptive practices, regulators are focused on protecting honest competitors, and in particular, not allowing companies that engage in dark patterns to gain market share through such patterns. Indeed, in its recent policy statement on unfair methods of competition, the FTC cited as an example of conduct that violates "the spirit" of the antitrust laws, "false or deceptive advertising or marketing which tends to create or maintain market power."[33]
- **General distrust of advertising/commercial practices:** Perhaps as a result of the ongoing techlash, regulators seem to increasingly distrust businesses and common commercial practices. This distrust is evidenced in some of the marketing that regulators themselves are using to describe companies and practices. Regulators increasingly characterize industry practices with a broad brush, in pejorative ways, from "junk fees," to "algorithmic discrimination," to "predatory lending" practices. Instead of "personalized advertising," they speak of "commercial surveillance." Instead of misleading advertising, they speak of "dark patterns."
- **Competition among regulators:** Typically, when one regulator highlights an important issue, others follow suit and look to regulations and guidance provided in other jurisdictions to develop their own policies. Given the speed with which dark patterns regulations, guidance, and advice have proliferated in the last few years, we can only imagine that additional regulators will want to get in on the action. Indeed, regulators are issuing new rules on dark patterns all the time. The California Age Appropriate Design Code will be effective on July 1, 2024 and prohibits businesses from using dark patterns that lead or encourage children to provide personal information beyond what is expected for an online service or product or that a business knows could be "materially detrimental" to the child's physical health, mental health, or well-being.[34] The Consumer Financial Protection Bureau has also gotten into the game: in January 2023, it issued guidance to "root out tactics which charge people fees for subscriptions they don't want."[35]

Given these considerations, it is clear that regulators are going to continue to focus on dark patterns. But where are they drawing the line as to what constitutes a dark pattern? How can companies that are merely engaging in traditional persuasive marketing techniques defend themselves against allegations that they are engaging in dark patterns? Here are some considerations:

30 See Joe Nocera, How Cookie Banners Backfired, N.Y. Times (Jan. 29, 2022), https://www.nytimes.com/2022/01/29/business/dealbook/how-cookie-banners-backfired.html (discussing that the proliferation of cookie banners may have had the opposite intended effect for consumers).

31 E.g. *In the Matter of PayPal, Inc., a corporation*, FTC Matter No. 1623102.

32 *AMG Capital Management, LLC v. FTC*, 141 S.Ct. 1341 (2021).

33 Fed. Trade Comm'n, Policy Statement Regarding the Scope of Unfair Methods of Competition Under Section 5 of the Federal Trade Commission Act (November 10, 2022), https://www.ftc.gov/legal-library/browse/policy-statement-regarding-scope-unfair-methods-competition-under-section-5-federal-trade-commission.

34 Cal. Civ. Code § 1798.99.31(b) (7).

35 Press Release, Consumer Financial Protection Bureau, CFPB Issues Guidance to Root Out Tactics Which Charge People Fees for Subscriptions They Don't Want (January 19, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-guidance-to-root-out-tactics-which-charge-people-fees-for-subscriptions-they-dont-want/.

- **While state privacy regulators may be able to impose certain requirements on privacy interfaces, the FTC can only take action against dark patterns that are unfair or deceptive.** A deceptive practice is one that is likely to mislead a consumer acting reasonably under the circumstances.[36] An unfair practice is one that causes or is likely to cause substantial injury that is not reasonably avoidable by consumers and not outweighed by benefits to consumers or competition.[37] It is not clear that, for example, nagging, "confirm shaming," or use of pre-checked boxes would be unfair or deceptive under these standards. Although states have broader discretion to take action against techniques that violate regulations, in the absence of federal legislation, the FTC would not have the authority to enforce these types of practices as deceptive or unfair.
- **Regulators should provide clearer guidance.** Although privacy regulations in California and Colorado provide examples of what might constitute dark patterns on privacy interfaces, it is unclear how the states will enforce these examples in practice. For example, Colorado prohibits use of "emotionally manipulative" language as part of a privacy choice interface. Would it be "emotionally manipulative" to say "I'd rather not exchange my data for free stuff"? Where will regulators draw the line?
- **First Amendment considerations:** Several researchers have discussed how certain "dark patterns" are likely protected under the First Amendment. One panelist at the FTC dark patterns workshop noted that, while dark patterns involving false statements would not likely be protected by the First Amendment, others, such as obstruction, nagging, or confirm shaming may well be protected.[38]

In short, while regulators may want to prevent design choices from nudging consumers into making purchases or privacy-invasive choices, there is a danger that their efforts could bleed into ordinary persuasion tactics commonly used in marketing. Restrictions on dark patterns cannot be justified simply because they are "too persuasive."[39] While regulators may have a greater interest in expanding their authority to define new categories of dark patterns, they are likely to be on more solid ground if they prioritize enforcement of traditionally unfair or deceptive dark patterns.

While businesses may need to push back on some of the edge cases, they would be well-advised to stick to the tried-and-true principles of advertising, marketing, and privacy claims that the FTC and other regulators have espoused for years, which include the following:

- **Don't make false claims.** These include false claims about prices, privacy, or product attributes. They also include false claims about scarcity, fake countdown clocks, or the like.
- **Make sure consumers authorize charges.** For example, companies should not trick consumers into paying for goods by mislabeling steps or including fees that are not clearly and conspicuously disclosed.
- **Comply with ROSCA and state auto-renewal laws when offering negative options:** Make sure the nature of a negative option service is clearly and conspicuously disclosed, that consumers provide express informed consent to being charged, and that cancellation is as easy as enrollment.
- **Disclose material information upfront.** Businesses should use plain, straightforward language to describe material information, and disclose the information clearly and prominently in the user flow in close proximity to any claims they are qualifying.
- **Pay special attention to state laws when developing privacy choice interfaces.** Privacy choices should be simple and understandable. They should also be symmetrical in that it should be just as easy to exercise a privacy protective choice as it is to provide data. Avoid double negatives and confusing toggles when describing and providing choices.
- **Pay special attention when your services are directed to children.** The FTC report on "Bringing Dark Patterns to Light" includes several examples where it is evident that there will be heightened scrutiny involving these services. Once the California Age Appropriate Design Code comes into effect, businesses will be prohibited from using dark patterns in their services that are likely to be accessed by children under the age of 18.

36 Fed. Trade Comm'n, FTC Policy Statement on Deception (October 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

37 15 U.S.C. 45(n).

38 Lior Strahilevitz, Fed. Trade Comm'n, "Bringing Dark Patterns to Light: An FTC Workshop" Transcript, at 75–76 (April 29, 2021), https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf.

39 *Sorrell v. IMS Health Inc.,* 564 U.S. 552, 578 (2011).

04
CONCLUSION

Companies that make claims directly to consumers, workers, and small businesses should review those claims to make sure that they are consistent with regulatory guidance. Where that guidance is unclear, companies will have to develop their own compliance policies based on their own risk analyses, customer considerations, and willingness to push back if regulators take issue with their claims.

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