Tech® REG CHRONICLE

DARK PATTERNS

MAY 2023

CPI COMPETITION POLICY® INTERNATIONAL

Competition Policy International, a What's Next Media and Analytics Company

LETTER FROM THE EDITOR

Dear Readers,

The term "dark patterns," though it may conjure up images of spycraft (or even black magic) refers to user interface ("UI") design techniques that are designed to manipulate and deceive users into taking courses of action that they might not have otherwise taken. The term was coined by Harry Brignull in 2010, a user experience consultant, and has gained increasing attention in recent years as a concern in the field of design ethics. They can take many forms, such as hiding important information, confusing users with misleading visuals or wording, or making it difficult to cancel or unsubscribe from a service. Such patterns are often used by companies to increase sales, gain more user data, or promote engagement on their platforms. Importantly, they can have negative impacts on user trust and satisfaction.

Although arguably the entire history of consumer protection law has been a story of combating dark practices in the physical world under different names, in recent years, there has been a growing explicit focus on the negative impact of dark patterns on user trust and behavior online. As a result, there have been several efforts to combat these deceptive practices. Perhaps most explicitly, in 2019, the U.S. Senate introduced the DETOUR Act (Deceptive Experiences To Online Users Reduction), which aims to prohibit the use of dark patterns and other deceptive design practices in online interfaces. This is reflected in other initiatives worldwide aiming at consumer protection. The articles in this Chronicle outline these efforts and their potential impact on the behavior of online firms towards their consumers.

To set the scene, **Maneesha Mithal & Stacy Okoro** provide an outline of the history of the regulation of dark practices, from its origin in classic consumer protection law, to more recent initiatives to counter such behavior online. The article helpfully sets out the concrete reasons why regulators are so focused on this issue at present, outlines the measures that regulators worldwide (notably in the U.S. and Europe) have been taking to tackle the issue, the potential limitations to these efforts, and the principles that online businesses should adhere to in order to avoid running afoul of this new wave of scrutiny.

Building on these themes, **Christine Chong & Christine Lyon** explore how regulators are increasingly looking beyond the terms of companies' privacy policies to scrutinize the structure of their user interfaces, websites, apps, and other

online services, and challenging concrete aspects of designs that potentially manipulate consumer choice through "dark patterns." The article examines the developing dark pattern regulatory enforcement landscape from a data privacy perspective, with a focus on recent U.S. and EU developments.

Looking specifically towards developments in the EU and the UK, **Katrina Anderson, Nick Johnson & Amelia Hodder** examine the EU's Unfair Commercial Practices Directive ("UCPD"), and the UK's Consumer Protection from Unfair Trading Regulations 2008 ("CPUT"). As the authors remark, these rules are increasingly being used by regulators to challenge dark patterns. In addition, dark patterns have also been challenged on the basis that they undermine the principles of the EU General Data Protection Regulations ("GDPR"), which remains in force in the UK post-Brexit. However, as the authors note, the law continues to be difficult to apply in the absence of practical guidance or a body of case law. The question therefore remains over when a given course of action by a business will cross the threshold from being a controversial marketing technique to being an illegal dark practice. In light of this, the authors query whether new legislation expressly outlawing dark patterns, notably the EU Digital Services Act and the EU Data Act, will finally provide more clarity on where the legal lines are to be drawn?

Turning again to the U.S., **Ryan C. Smith** discusses how the Federal Trade Commission is ramping up its enforcement in this regard. $350 million in settlements were announced in late 2022 relating to dark patterns. Nevertheless, many businesses may be uncertain as to what dark patterns exactly are, or may think they are immune. The authors emphasize that the FTC's enforcement practices are industry-agnostic and derived from previous enforcement actions over the last decade. By examining these current and past trends, the authors elaborate a set of best practices for UI design that do not present unnecessary hurdles to consumers.

Advocating for a slightly more cautious approach, **Victoria de Posson** acknowledges the widespread consensus that design practices involving psychological manipulation and deceit should be banned. However, rather than more legislation, the author underlines the key challenge of developing clear guidance based on robust research of what might constitute a dark pattern, assessing on a case-by-case basis the real impact and intention behind a practice. She warns that regulators should not go for the easy way out and standardize online interfaces, noting that in Europe, there is a well-developed *acquis* of consumer law addressing "dark patterns" both online and offline. Instead of adding another layer of rules, the author argues that policymakers should focus on better and more consistent enforcement of what is in place already.

Indeed, as **Frédéric Marty & Jeanne Torregrossa** argue, although the concerns discussed above demonstrate that there is a legitimate concern surrounding dark patterns, there are a certain number of risks and limits that need to be taken into consideration in terms of public policy design. For example, personalization is not a competitive problem as such. Personalized recommendations, especially based on algorithmic predictions grounded on massive data collection and processing, can contribute to economic efficiency and consumer satisfaction. Secondly, "dark patterns" are not the exclusive privilege of dominant digital firms. They may be implemented in brick-and-mortar stores (albeit with less efficiency and refinement). They can also be implemented by non-dominant operator. While it is therefore legitimate to be concerned about dark patterns, possible remedies should be carefully considered.

In sum, the recent initiatives to regulate "dark patterns" mark important steps towards ensuring a fair and transparent digital environment. As **Kyle R. Dull & Julia B. Jacobson** underline, it will be key for all players to maintain awareness of the different types of dark patterns and to take steps to protect their businesses by focusing on offering consumers the information and experience needed to make fully informed decisions.

While the complexity of the issue poses challenges for regulators and businesses alike, it is clear that the issue cannot be ignored. With more countries and organizations joining the effort to combat this issue, regulators hope to see greater accountability and responsibility from businesses in the future. All underline the need to continue monitoring and evaluating the effectiveness of these regulations, and to remain vigilant against new forms of deceptive design practices that may arise, and, perhaps most importantly, all prioritize user autonomy and trust.

As always, many thanks to our great panel of authors.

Sincerely,
CPI Team

TABLE OF CONTENTS

CPI COMPETITION POLICY® INTERNATIONAL

DARK PATTERNS

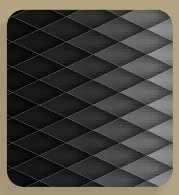
MAY 2023

SUMMARIES

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.



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.

DARK PATTERNS – A EUROPEAN REGULATORY PERSPECTIVE

By Katrina Anderson & Nick Johnson

Dark Patterns are deceptive and manipulative features of a user interface that push or nudge consumers into making certain choices that are not in their best interests. Such features are increasingly catching the eye of consumer and data protection regulators across Europe, including in the UK, the EU and beyond. However, considerable uncertainty remains over their legality and indeed their definition itself. The EU's Unfair Commercial Practices Directive ("UCPD") at an EU level, and Consumer Protection from Unfair Trading Regulations 2008 ("CPUT") in the UK are increasingly being used by have allowed regulators to begin to challenge the fairness of the application of dark patterns. Dark patterns have similarly challenged on the basis they been shown to undermine some of the principles of the General Data Protection Regulations ("GDPR"). However, the law continues to be difficult to apply in the absence of practical guidance or a body of case law. The question therefore remains over when a dark pattern will cross the threshold from divisive marketing technique to illegal practice. With new legislation expressly outlawing dark patterns [,notably the EU Digital Services Act and the EU Data Act,] on its way, will this provide more clarity on where the legal lines are drawn?

DARK PATTERNS DEFINED: EXAMINING FTC ENFORCEMENT AND DEVELOPING BEST PRACTICES

By Ryan C. Smith

The Federal Trade Commission is ramping up its enforcement of so-called dark patterns, with $350 million in settlements announced in late 2022. Many businesses may be uncertain what dark patterns are, or may think they do not need to worry. This Article argues that the FTC’s enforcement practices are industry-agnostic and derived from previous enforcement actions over the last decade. By examining these current and past enforcement actions, it is possible to develop a set of best practices around robust user notice and choice and user interface designs that do not present unnecessary hurdles to consumers.

DARK PATTERNS: PROTECTING CONSUMERS WITHOUT HINDERING INNOVATION

By Victoria de Posson

There is a widespread consensus that design practices involving psychological manipulation and deceit should be banned. However, when it comes to defining the concept of "dark patterns," the challenge is to identify the line that separates legitimate user interface design from deceptive practices. It is crucial to have clear guidance based on robust research of what might constitute a dark pattern, assessing on a case-by-case basis the real impact and intention behind a practice. It is important to distinguish online persuasive design practices from deceptive ones to ensure the same commercial rights are granted to online businesses as to brick-and-mortar ones. Any initiative must be limited to "dark patterns" that are illegitimate. Regulators should not go for the easy way out and standardize online interfaces. A one-size-fits-all approach would not work for the variety of online services and harm competition among similar brands. In Europe, there is a well-equipped *consumer acquis* addressing "dark patterns." Instead of adding another layer of measures, policymakers should focus on better and more consistent enforcement of existing rules.

DARK PATTERNS AND MANIPULATION

By Marcela Mattiuzzo

The term "dark patterns" became popular and has gained much attention from both enforcers and academics. It connects strictly to behavioral studies and the relevance of choice architecture, notably in the online environment. If dark patterns entail the deployment of choice architecture in ways that misguide individuals and that may lead to harm, one relevant question in this discussion is assessing whether the mere fact that some form of manipulation is being deployed would mean the practice should be deemed unlawful. This article proposes that though the discussion on the legality of manipulation is relevant – and the definition of what is considered to be manipulative is paramount – the dark patterns debate gains more by focusing on the impact of dark patterns' deployment for individuals.

UNCLOAKING DARK PATTERNS: IDENTIFYING, AVOIDING, AND MINIMIZING LEGAL RISK

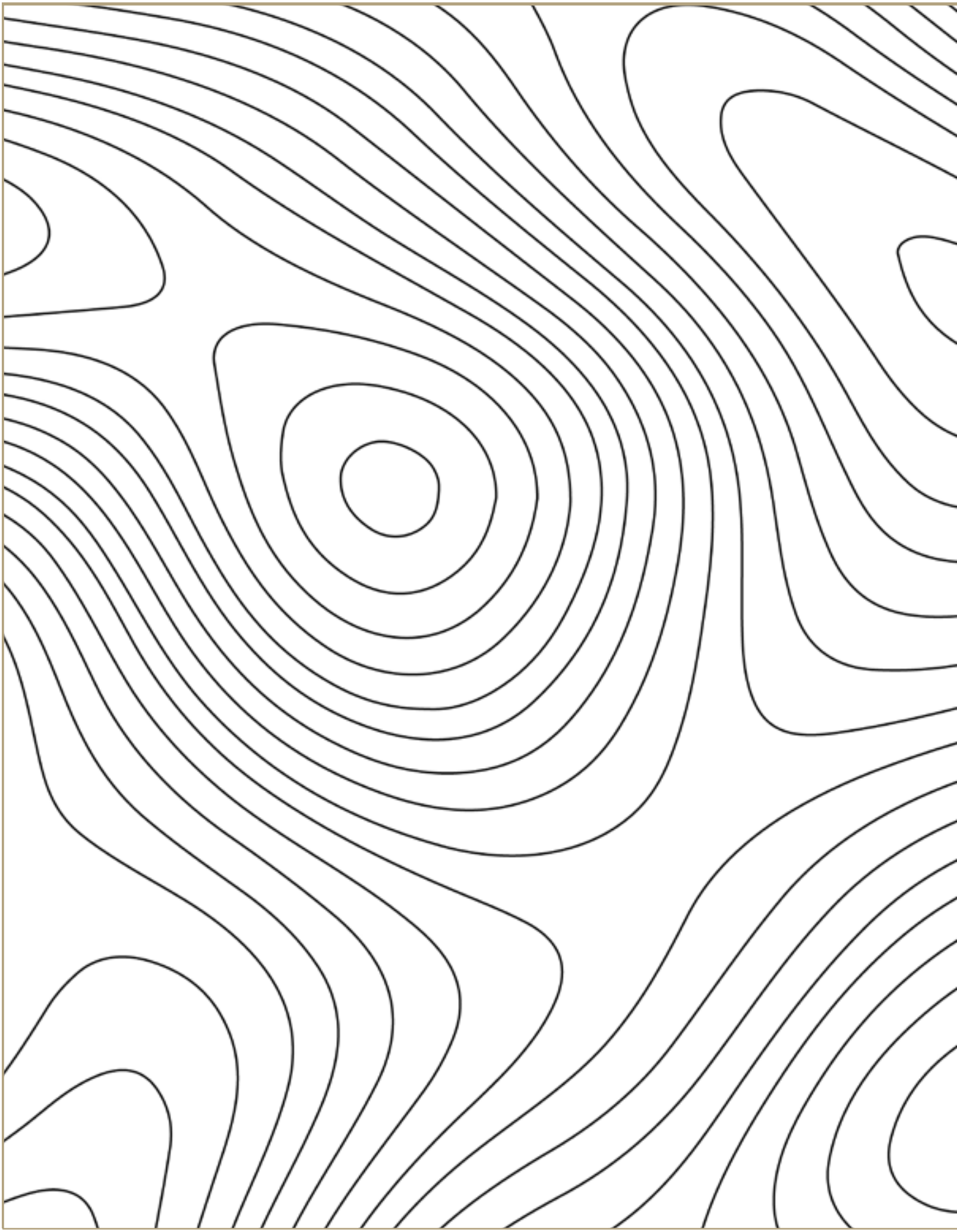
By Kyle R. Dull & Julia B. Jacobson

Regulators have long targeted deceptive and misleading practices designed to manipulate consumers, including more recently "dark patterns." Dark patterns are misleading or otherwise manipulative user experiences intended to influence a consumer's behavior and prevent them from making fully informed choices. Dark patterns are not merely clever marketing gimmicks; rather, they are designed to cause users to unwittingly act against their personal preferences, such as signing up for services they do not want, purchasing products they do not intend to purchase, sharing personal information. In this article, we review common dark patterns and how they are used in today's digital world. We also analyze consumer protection and privacy regulatory developments targeting dark patterns and discuss best practices for digital service operators to help minimize regulatory sanctions, class actions and reputational damage arising from dark pattern practices.

TACKLING DARK PATTERNS: HOW TO REASONABLY PREVENT CONSUMER MANIPULATION AND COMPETITION DISTORTIONS?

By Frédéric Marty & Jeanne Torregrossa

Deceptive and manipulative choice architectures have received significant coverage in the academic literature. These dark patterns can be nudges leading individuals to act against their interests or sludges hindering the implementation of beneficial decisions. The development of these patterns is enhanced by the potential of the data economy and by ever more powerful predictive algorithms. They raise legitimate concerns in terms of competition and consumer protection. Numerous reports suggest the introduction of regulatory measures that should be assessed based on their possible effects. This contribution shows that while these measures are necessary, it is important to emphasize that dark patterns are not the privilege of dominant operators and preventing them should not preclude the net gains that can result from the personalization of algorithmic recommendations. Dark patterns, acknowledged as manipulative practices, have been fiercely debated during the Digital Services Act negotiations. They are added to the already long list of issues facing the digital economy. But what exactly is behind them?



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.

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

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

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 connection 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 Cali-

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.

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).

fornia 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

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]

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.

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

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 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]

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.

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.

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 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

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.

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]

> *"As a result, the FTC has been searching for alternative ways to get monetary relief and impose monetary penalties*

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:

- **While state privacy regulators may be able to impose certain requirements on privacy interfaces, the FTC can only take action against dark patterns that**

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/.

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.

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.

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).

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

BY
CHRISTINE CHONG

&
CHRISTINE LYON

Freshfields Bruckhaus Deringer U.S. LLP.

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

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/.

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]

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

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 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]

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.

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.

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

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.*

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

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

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.

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*

DARK PATTERNS – A EUROPEAN REGULATORY PERSPECTIVE

BY KATRINA ANDERSON

& NICK JOHNSON

& AMELIA HODDER

Katrina Anderson is an associate director, Nick Johnson, a partner, and Amelia Hodder, a trainee solicitor, at Osborne Clarke. an international legal practice headquartered in London.

01 INTRODUCTION TO DARK PATTERNS

Dark patterns is a term that refers to deceptive and manipulative features of a user interface ("UI") that push or nudge people into making choices that are not in their best interests.

While concern about dark patterns is growing amongst European consumer and data protection regulators, there is still considerable uncertainty over when the use of dark patterns will cross the threshold from persuasive marketing technique to illegal practice.

As the e-commerce world has become more sophisticated, businesses have developed more and more innovative methods to influence consumer choices, culminating in a perception that there is a culture of "dark pattern" usage. Reg-

ulators in Europe typically take the view that consumers encountering dark patterns on retailer websites may end up, for example, purchasing items more quickly and with less consideration than intended, or entering into subscriptions and being unable to cancel them. Data protection regulators are concerned that dark patterns may coax users into inadvertently consenting to the processing of their personal data or accepting more privacy-intrusive settings than they otherwise might.

Despite being a major concern for European regulators, dark patterns did not start as a legal concept and as a result they are not clearly or consistently defined. For example, the newly enacted EU Digital Services Act (the "DSA")[2] refers to them as practices on the UI that "materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions."[3] Similarly the EU's proposal for the Data Act[4] views dark patterns as "design techniques that push or deceive consumers into decisions that have negative consequences for them."[5] In subtle contrast, the guidelines of the European Data Protection Board (the "EDPB") on dark patterns in social media platform interfaces[6] consider dark patterns themselves to be a form of UI or user experience[7] and deem the decisions that users are pushed into regarding their personal data to be "unintended, unwilling and potentially harmful."[8]

Adding further uncertainty are the multiple typologies of dark pattern and variations in their names. Recently, the UK's Consumer and Markets Authority (the "CMA") flagged 21 potentially harmful forms of "Online Choice Architecture" (which is the term the CMA and Dutch regulator[9] use for dark patterns) practice, divided into three categories; those affecting choice structure (the design and presentation of options), choice information (the content and framing of information provided), and choice pressure (through indirect influence of choices).[10] It has pinpointed the dark patterns it considers "almost always harmful" as "choice overload and decoys," "sensory manipulation," "sludge," "dark nudge," "forced outcomes," "drip pricing," "complex language," and "information overload."[11]

Adding further uncertainty are the multiple typologies of dark pattern and variations in their names

In January this year the European Commission announced the results of a sweep by the Consumer Protection Cooperation (the "CPC") of 399 retail websites which showed that nearly 40 percent were using "manipulative online practices to exploit consumer vulnerabilities or trick them."[12] The sweep focused on the following dark patterns: fake countdown timers; web interfaces designed to lead consumers to purchases, subscriptions or other choices; and hidden information.

Our review of the different typologies and naming conventions suggests that while there is a lack of consensus about the names of the different dark patterns themselves, dark patterns can broadly be broken down into nine themes:

1. Pressure – repeatedly being asked to act or confronted with (alleged) social norms or scarcity of goods.
2. Force – users are (*de facto*) forced to take action or acquiesce to do something.
3. Obstacles – users face various obstacles to dissuade them from taking certain actions.
4. Sneaking – additional purchases or goods or ser-

2 European Council Regulation No. 2022/2065, 2022 O.J (L 277/1) (Digital Services Act).

3 *Ibid*. at Recital 67.

4 Proposal for European Council Regulation on harmonised rules on fair access to and use of data No. 2022/0047(COD), 2022 COM(2022) 68 final (Data Act Proposal).

5 *Ibid.* at Recital 34.

6 European Data Protection Board, Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them, 3/2022 1. (March 14, 2022). https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf.

7 *Ibid.* at page 7.

8 *Ibid.*

9 Netherlands Authority for Consumers and Markets (ACM).

10 Competition and Markets Authority, Discussion Paper, *Online Choice Architecture: How digital design can harm competition and consumers,* CMA155 (April 2022). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf.

11 *Ibid.*

12 Press Release, European Commission, Consumer protection: manipulative online practices found on 148 out of 399 online shops screened (Jan. 30, 2023), (IP/23/418) https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418.

vices are imposed on users.
5. Deception and misdirection – the UI is created to distract from relevant information or to frustrate the usual expectations of the UI design.
6. Overloading – users are faced with an avalanche of requests, information, options or possibilities in order to prompt them to make certain choices.
7. Hindering – the obstruction or blocking of users from becoming informed or being able to make certain choices.
8. Fickle – UI design that is inconsistent or not clear, making it hard for the user to navigate to make the choices they want to make.
9. Left in the dark – UI designed to hide information or choices.

We consider that individual dark patterns can then be categorized within these themes. For example, confirm-shaming (where the UI attempts to make the user feel guilty for selecting their preferred option) and limited stock notifications sit within "Pressure." "Roach motels" (subscription traps with numerous barriers to cancel, making cancellation significantly harder than signing up) would come under "Obstacles."

Currently "roach motels," pre-selection of advantageous choices and false timers seem to be drawing particular attention in Europe.

02
REGULATION OF DARK PATTERNS

The concept of reducing friction and optimizing UI design has been around for many years. Even the idea that consumers might be "nudged" into certain choices is not new. Consumer protection and data protection law have always applied to UI design as much as to other aspects of businesses' interactions with consumers. However, it is only recently that European regulators and legislators have used the term "dark patterns" and specifically called out how consumer protection and data protection law should regulate these practices.

Increasingly dark patterns are explicitly mentioned and expressly outlawed in new and proposed legislation, such as in the DSA.[13] Further, the EU's public consultation as part of the Fitness Check of EU consumer law on digital fairness[14] clearly had dark patterns in mind when it probed respondents on whether: they had experienced websites designed to pressure them to purchase and make them uncertain of their rights and obligations; they had encountered difficulties cancelling subscriptions; and they would agree that stronger protections against "digital practices that unfairly influence consumer decision-making"[15] were required.

A. Consumer Law

The use of dark patterns can contravene the Unfair Commercial Practices Directive[16] (the "UCPD") at an EU level, which is mirrored in the UK by Consumer Protection from Unfair Trading Regulations 2008 ("CPUT").[17] These prohibit unfair commercial practices, including practices that amount to misleading actions or omissions, that are aggressive or that use harassment, coercion or undue influence. A commercial practice is also unfair under this legislation if it is "contrary to the requirements of professional diligence"[18] and "it materially distorts or is likely to materially distort the economic behavior with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers."[19] Guidance on the UCPD from the European Commission[20] expressly states that it can be utilized to challenge the fairness of the application of dark patterns in business-to-consumer commercial relationships and suggests, for example, that confirm-shaming could amount to an "aggressive practice using undue in-

13 Digital Services Act, *supra* note 2, at Article 25.

14 European Commission, Consultation, *Digital fairness – fitness check on EU consumer law* https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law/public-consultation_en.

15 *Ibid.*

16 European Council Directive No. 2005/29, 2005 O.J (L 149/22).

17 The Consumer Protection from Unfair Trading Regulations 2008, SI No. 2008/1277.

18 Unfair Commercial Practices Directive, *supra* note 16 at Article 3(2)(a).

19 *Ibid.* at Article 3(2)(b).

20 European Commission, 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, 2021O.J. (C 526/1) (Guidance on the Unfair Commercial Practices Directive).

fluence to impair the consumer's decision-making."[21] It also sets out the practices often recognized as dark patterns that are caught by the list of so-called "blacklisted offences" – commercial practices that are always considered unfair under the UCPD (which is also replicated in CPUT).

The "blacklisted offences" under the UCPD and CPUT include, for example, "[f]alsely stating that a product will only be available for a very limited time, or that it will only be available on particular terms for a very limited time, in order to elicit an immediate decision and deprive consumers of sufficient opportunity or time to make an informed choice."[22] It is easy to see how the use of countdown timers, a "Pressure" dark pattern, could fit within this if they are counting down to the expiry of a sale or deal which will not in fact end when the timer ends and are therefore false. This is endorsed by the European Commission's guidance on the UCPD[23] and the CMA also took this view when it announced at the end of 2022 that it would be examining whether the mattress-in-a-box company, Emma Sleep, had misled consumers by using countdown timers that implied a discount would end, when this was potentially not the case.[24] This investigation by the CMA forms part of its Online Choice Architecture program to tackle potentially harmful online selling practices.

Even if the practices targeted are not always expressly referred to as "dark patterns," there has been significant enforcement across Europe under consumer protection legislation. An early example of regulation of dark patterns under the UCPD is the Italian Competition Authority's ("AGCM") decision to fine two online travel operators for using practices that hindered consumers' ability to view all of the relevant information on additional costs attached to the purchase.[25] It also found the automatic pre-selection of an optional insurance policy misled consumers into believing this was compulsory. The AGCM in general has been active in its use of consumer law to regulate dark patterns. More recently, the Norwegian Consumer Council has written to various platform hosts alleging the use of dark patterns in their interfaces.

Even if the practices targeted are not always expressly referred to as "dark patterns," there has been significant enforcement across Europe under consumer protection legislation

Further, The CPC's sweep of dark patterns in relation to e-commerce and the call for European consumer protection regulators to contact e-commerce websites which have been identified as featuring dark patterns[26] may very well lead to enforcement. The CMA also announced that the *Emma Sleep* investigation would be the first of its investigations in relation to Online Choice Architecture[27] and therefore further action is anticipated in the UK in the coming months.

B. Data Protection Law

The "fair processing" principle in Article 5(1)(a) of the General Data Protection Regulation ("GDPR")[28] requires that data be processed "fairly and in a transparent manner."[29] The EDPB has also stated that "fairness is an overarching principle which requires that personal data shall not be processed in a way that is unjustifiably detrimental, discriminatory, unexpected or misleading to the data subject."[30] Arguably, therefore, if a UI uses dark patterns to facilitate insufficient or misleading information in respect of the processing of data for the user, this will necessarily amount to unfair processing. Additionally, where

21 *Ibid.* at 4.2.7.

22 Unfair Commercial Practices Directive, *supra* note 16 at Annex 1 and The Consumer Protection from Unfair Trading Regulations, *supra* note 17 at Schedule 1 .

23 Guidance on the Unfair Commercial Practices Directive, *supra* note 20 at 4.2.7.

24 Press Release, Competitions & Markets Authority, CMA investigates online selling practices based on 'urgency' claims (November 30, 2022) https://www.gov.uk/government/news/cma-investigates-online-selling-practices-based-on-urgency-claims.

25 Press Release, Italian Competition Authority, PS7488-PS7245 - Air transport: Antitrust fines Ryanair and EasyJet for more than a million euro due to misleading practices in the travel insurance (February 17, 2014) https://en.agcm.it/en/media/press-releases/2014/2/alias-2105.

26 ttps://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/sweeps_en#:~:text=2022%20%E2%80%93%20sweep%20on%20dark%20patterns,-Manipulative%20practices%20called&text=The%20CPC%20authorities%20decided%20to,products%20for%20their%20own%20account.

27 CMA investigates online selling practices based on 'urgency' claims, *supra* note 24.

28 European Commission Regulation No. 2016/679, 2016 O.J. (L119) (GDPR).

29 *Ibid.* at Article 5(1)(a).

30 European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 2. (October 20, 2020) 3.3 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

consent is the lawful basis for the processing of personal data, the GDPR requires this to be "given freely, informed and unambiguous"[31]. Dark patterns employed to push users to agree to give away more personal data than necessary (such as nagging and continuous prompting – forms of "Pressure" dark pattern) may render such consent invalid.

Article 25 of the GDPR additionally imposes an obligation on data controllers to practice data protection by design and default.[32] EDPB guidance explains that the fairness elements of design and default include an absence of deception, specifically "[d]ata processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design."[33] It is again likely that using dark patterns, such as a false hierarchy (for example a green "reject" button and red "accept" button) or confirmshaming, could undermine the Article 25 requirements.

Enforcement action has already been taken under the GDPR to regulate dark patterns. For example, the Court of Justice of the European Union held that the automatic pre-selection of checkboxes, a form of "Obstacles" dark pattern, by an online lottery service did not provide valid consent for the use of cookies or similar technologies.[34] This practice was held to be in breach of the GDPR as consent was not freely given.

Recent guidance by the EDPB on dark patterns in social media platform interfaces[35] is another example of the increased attention in this area on the part of regulators, and sheds some further light on the relationship between use of dark patterns and GDPR compliance. It calls for national regulators to sanction dark patterns that breach the GDPR and provides examples of best practice for various parts of the social media interface in contrast to illustrations of potentially illegal use of dark patterns. While the guidelines focus on social media platforms – a perennial target of European data protection regulators – its principles would generally seem to be equally applicable to other online UIs.

03

WHEN ARE DARK PATTERNS UNLAWFUL? – A LACK OF CERTAINTY UNDER THE LAW

As the concept crystalizes, it is becoming easier to understand which features of the UI raise concerns and might amount to a dark pattern. However, what remains less clear is exactly when a dark pattern will cross the line into being unlawful. There is now no doubt that dark patterns *can* amount to a breach of consumer and data protection laws, but the grey area over when exactly this threshold is crossed is problematic for businesses seeking to achieve compliance.

A. Principles-Based Laws and an Absence of Clear Guidance and Case Law

The issue legally is that Europe's principles-based consumer protection and privacy laws are only lightly tested in relation to dark patterns. The principal sources of dark patterns regulation, the UCPD, CPUT and the GDPR, have a wealth of case law and guidance in relation to unfair commercial practices and what is required for data protection respectively but these are largely not directly relevant to dark patterns or apply only by analogy.

There is some guidance, for example, as discussed above the EDPB released guidelines on dark patterns in social media platform interfaces.[36] The European Commission's guidance on the UCPD[37] also makes express reference to dark patterns and the CMA has published research (but not guidance) into Online Choice Architecture.[38] The European Commission's guidance notes the ability of businesses to use data to create persuasive practices that are personalized to the consumer

31 *Ibid.* at Article 4.

32 *Ibid.* at Article 25.

33 European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, *supra* note 28 at 3.3.

34 Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH*, 2019 O.J. C 112.

35 European Data Protection Board Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them, *supra* note 6.

36 *Ibid.*

37 Guidance on the Unfair Commercial Practices Directive, *supra* note 20 at 4.2.7.

38 Competition & Markets Authority, *Online Choice Architecture: How digital design can harm competition and consumers*, (Discussion Paper CMA155, April 2022) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf and Competition & Markets Authority, Evidence review of Online Choice Architecture and consumer and competition harm (Evidence Review CMA157, April 2022) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1069423/OCA_Evidence_Review_Paper_14.4.22.pdf.

and to continually adjust such practices to improve their effectiveness, observing that often such practices are employed without consumers' full knowledge.[39] It also raises concerns about A/B testing. However, this is all expressed in terms of generalities and concerns generally about "opaqueness," [40] which in practice means that it is still hard to apply in a way that allows businesses to distinguish persuasive advertising or sales techniques from potentially manipulative commercial practices that are unfair under consumer law.

To illustrate the issues, take the example of an offer presented to a consumer attempting to cancel their subscription that provides 50 percent off the next 3 months if they choose to abandon cancellation. There are relatively strong arguments to support that this could be a dark pattern. It could be caught under the headings of Obstacles (for example as part of a roach motel) or Hindering (by prolonging the cancellation process by questioning the user's choice). There is, however, very little guidance or case law that provides a steer on whether this dark pattern (if it is such) is also contrary to the UCPD or CPUT or any other laws. There is nothing in the law that prescribes how cancellation of a subscription is to be achieved.

> ***There is some guidance, for example, as discussed above the EDPB released guidelines on dark patterns in social media platform interfaces***

Certainly, preventing a consumer from exercising their legal rights to cancel a contract is highly problematic but what about presenting the consumer with an offer to keep the subscription at a discount? This is clearly a barrier to cancellation but is it a sufficient barrier such that it is tantamount to preventing the consumer from exercising their rights of cancellation under the contract or their statutory right of withdrawal? Much will ultimately depend on how it is presented to the consumer and how easy it is in practice for that consumer to navigate around the offer and finally cancel their contract. The offer to keep the subscription might also be an unfair commercial practice or misleading under the UCPD or CPUT, but this is likely to hinge on how comparatively prominent the option to cancel is and how easy it would be for the consumer to exercise their cancellation rights. While some of the commentary in this area creates the impression that symmetry between the ease of sign up and cancellation is required in relation to subscriptions, there is at the time of writing no obvious basis for this in law.

Undoubtedly, case law and guidance will develop over time, but in the meantime, businesses are faced with difficult decisions in weighing up the risk of enforcement action, which may have the potential to cause serious reputational damage alongside potential fines and/or criminal law sanctions, against the advantages of designing their platforms so as to optimize sales and the communication of offers and deals to customers.

B. Incoming Legislation Doesn't Quite Add Enough Color

The DSA, which will apply to online platforms, will be the first piece of EU legislation that expressly bans dark patterns. However, the ban will only operate where existing laws on unfair commercial practices and the GDPR do not apply. It gives non-exhaustive examples of specific practices, such as subscription traps and giving more prominence to certain choices when asking a recipient of the service for a decision.[41] The DSA's explicit ban on dark patterns, on its face, should close a loop as it catches any use of dark patterns that is not in breach of the UCPD and the GDPR. However, two key challenges exist. The first is establishing whether the dark patterns in question are caught by one or other of these pieces of legislation. The second is applying the DSA's test of something that "deceives, manipulates or otherwise materially distorts a user's ability to make an informed decision."[42] This will be challenging without further guidance on how this is expected to be applied in practice. The DSA threatens large fines[43] which are surely intended to incentivize compliance, yet their deterrent effects may be hindered by a lack of clarity in respect of the DSA's jurisdiction over dark patterns.

That said, although we do not anticipate much actual enforcement under the DSA, it is significant that the EU considers dark patterns to be worthy of an express prohibition and this perhaps sets the tone for future enforcement and bans under the UCPD, CPUT or the GDPR given that the European Commission's stated view that these pieces of legislation are capable of capturing most dark patterns.[44]

39 Guidance on the Unfair Commercial Practices Directive, *supra* note 20 at 4.2.7.

40 *Ibid.* at 4.2.6.

41 Digital Services Act, *supra* note 2, at Article 25(3).

42 Digital Services Act, *supra* note 2, at Article 25(1).

43 *Ibid.* at Article 53.

44 https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418.

The DSA is not the only place where we are seeing proposals to outlaw dark patterns in Europe. The EU's recently presented Data Act proposal[45] explicitly prohibits dark patterns. The most recent draft accepted by the Parliament applies to the manufacturers of connected products and providers of related services which are placed on the market in the EU and governs rights and obligations regarding the data generated by the use of the products and services. It sets out that data holders or third parties who receive the data of the user of the products or recipient of services from a data holder at the request of that user, are not to subvert or impair the autonomy of users to "coerce, deceive or manipulate" them in any way and therefore they should not use dark patterns in the design of the digital interface.[46] The Data Act proposal also states "[c]ommon and legitimate commercial practices that are in compliance with Union law should not in themselves be regarded as constituting dark patterns."[47]

Also proposed by the European Commission is the Artificial Intelligence (AI) Act[48] which incorporates what may be read as a limited prohibition on certain kinds of dark patterns. Under this draft legislation, "Prohibited Artificial Intelligence Practices" include AI systems that "deploy subliminal techniques"[49] or that exploit the vulnerabilities of a "specific group of persons due to their age, physical or mental disability"[50] with the intention to materially distort their behavior and in a manner that causes or is likely to cause physical or psychological harm to that person or another.[51] This prohibition appears to have a relatively high threshold in order to be engaged as a result of the requirement that the distortion of behavior must be intended and "material," and the need for harm to be "physical or psychological harm." The UK has also looked at this issue as part of the UK consumer law refresh[52] which, at the time of writing, is still in progress and the draft Digital Markets Competition and Consumer Bill which is expected imminently. The UK government's approach appears to be that they will mirror the EU by commissioning further research and are contemplating an express ban – although this is not expected in the Bill.

In summary, dark patterns are high on the legislative and enforcement agenda in Europe. However, the law continues to be difficult to apply in the absence of practical guidance or a body of case law. It is also likely that deviations in the application of these laws will emerge across Europe as regulators attempt to utilize them to regulate dark patterns, which could result in certain forms of dark pattern being regarded as nothing more than a marketing technique in one jurisdiction but unlawful in another.

04
CONCLUSION

Recent activity such as the CPC sweep, the wave of letters from the Norwegian Consumer Council and the CMA's Online Choice Architecture Programme confirm that dark patterns are attracting considerable regulatory attention in Europe. No doubt enforcement will result and with this will come with publicized decisions that provide some clarity on where the legal lines are drawn. As new legislation outlawing dark patterns is introduced we can hope to see accompanying guidance or test cases that offer better insight into what this means for businesses who operate online interfaces and want to market effectively, but compliantly, to their customers.

The DSA is not the only place where we are seeing proposals to outlaw dark patterns in Europe

45 Data Act Proposal, *supra* note 4 at Recital 34.

46 *Ibid.* at Article 6(2).

47 *Ibid.* at Recital 34.

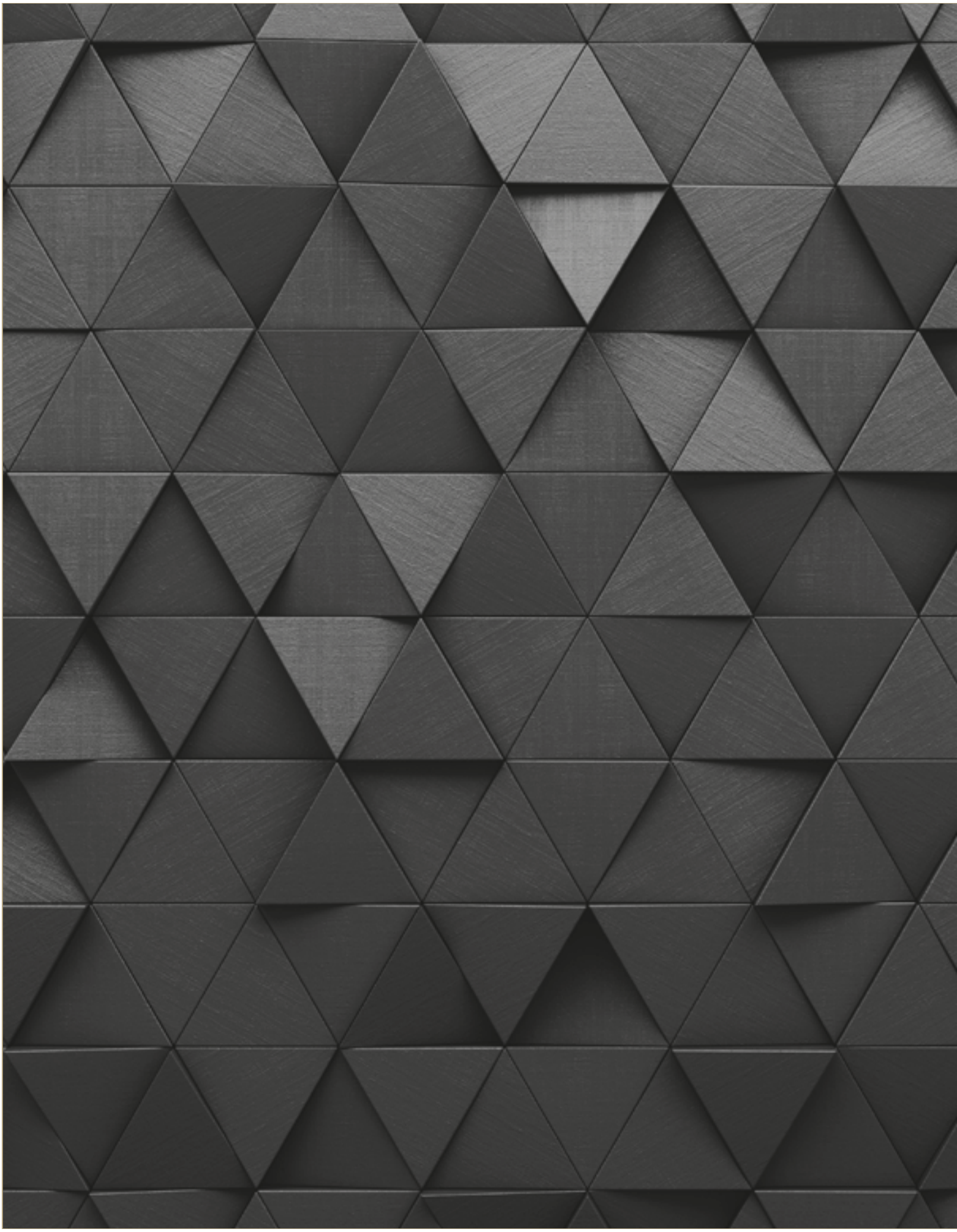
48 Proposal for European Council Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts No. 2021/0106 (COD), 2021 COM(2021) 206 final (AI Act Proposal).

49 *Ibid.* at Article 5.

50 *Ibid.*

51 *Ibid.*

52 Department for Business, Energy and Industrial Strategy, Consultation outcome – Reforming competition and consumer policy: government response (CP 656, April 20, 2022) https://www.gov.uk/government/consultations/reforming-competition-and-consumer-policy/outcome/reforming-competition-and-consumer-policy-government-response.



DARK PATTERNS DEFINED: EXAMINING FTC ENFORCEMENT AND DEVELOPING BEST PRACTICES

BY
RYAN C. SMITH

Ryan Smith is Counsel for Compliance and Policy at the Network Advertising Initiative, the leading self-regulatory organization for the ad tech industry. He regularly counsels member organizations on best practices for data privacy and consumer choice.

In late 2022, the Federal Trade Commission ("FTC") announced settlements with two different businesses over the use of so-called "dark patterns." Defining dark patterns is complicated; the FTC's definition ("design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm") does not provide much enlightenment.[2] But using dark patterns can be costly: the first settlement in 2022 was a $100

2 Fed. Trade Comm'n, Bringing Dark Patterns to Light (Sept. 2022) at 2.

million settlement with Vonage Holdings, a cloud communications provider.[3] The second was a $245 million settlement with Epic Games, Inc., maker of the popular video game Fortnite.[4] While these two enforcement actions represented the first time the FTC specifically named dark patterns in a complaint, they were not harbingers of an unexpected sea change. In 2021, the FTC held a workshop on "Bringing Dark Patterns to Light," signaling an interest in dark patterns.[5] The complaints against both Vonage and Epic are also not treading new ground; while the FTC names dark patterns in both complaints, the foundations of the FTC's arguments can be found in other, older enforcement actions.

The FTC is not the only enforcement agency eyeing dark patterns. Eighteen state attorneys general wrote to the FTC in August 2022, urging more action be taken on dark patterns.[6] The State of California, with its expansive California Privacy Rights Act ("CPRA"), outlaws the use of dark patterns when obtaining consumer consent for the collection of personal information.[7] Colorado, in the Colorado Privacy Act ("CPA"), and Connecticut, in the Connecticut Data Privacy Act ("CTDPA") do as well.[8] With $345 million in settlement payments (and counting), every business that interacts with consumers ought to be aware of dark patterns and how to avoid them.

One hurdle businesses face, beyond assessing their consumer-facing communications and interactions, is defining what dark patterns are. The FTC's definition asks more questions than it answers. The CPRA is likewise not forthcoming ("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 definitions found in the California Privacy Protection Agency's proposed regulations can only define dark patterns by what they are *not*.[10] Colorado's definition largely mirror's the FTC's.[11] Connecticut, meanwhile, just defers to the FTC.[12]

Companies across a diverse array of industries are scrambling to ensure compliance with vague directives in state law and in federal regulations. Without much guidance, it almost seems easier for legal teams to shrug their shoulders. But it is possible to discern patterns in previous FTC enforcement actions that can guide businesses as they carefully scrutinize their interactions with consumers. The FTC's dark patterns jurisprudence (if it can be called that) is not only identifiable but is easy to distill. This Article gives a brief overview of the FTC's enforcement actions against both Vonage and Epic Games, and then examines previous enforcement actions dating back to the mid-2010s to develop a set of recommended best practices that are agnostic to industry and business model and focus on straightforward interactions with consumers online.

01

ANALYZING *VONAGE* AND *EPIC GAMES*

For a company that serves digital ads on online publications, or a company that makes a weather app, it can seem unintuitive to look at enforcement actions against a cloud

3 Press Release, Federal Trade Commission, FTC Action Against Vonage Results in $100 Million to Customers Trapped by Illegal Dark Patterns and Junk Fees When Trying to Cancel Service (Nov. 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.

4 Press Release, Federal Trade Commission, Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges (Dec. 19, 2022) https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations.

5 Lesley Fair, *Bringing Dark Patterns to Light*, Business Blog (Feb. 24, 2021), https://www.ftc.gov/business-guidance/blog/2021/02/bringing-dark-patterns-light.

6 See Letter from Kwame Raoul, Illinois Attorney General, to Matthew Ostheimer, Bureau of Consumer Protection, Fed. Trade Comm'n (Aug. 22, 2022) https://illinoisattorneygeneral.gov/pressroom/2022_08/17%20Attorneys%20General%20Hawaii%20OCP%20Digital%20Advertising%20P114506%20FTC%202022-0035-0001.pdf.

7 See Cal. Civ. Code § 1798.140(h) (2023) ("[A]greement obtained through the use of dark patterns does not constitute consent.").

8 See Col. Rev. Stat. § 6-1-1303(5)(c) (2023); Conn. Gen. Stat. § 42-515(6)(C) (2023).

9 Cal. Civ. Code § 1798.140(l) (2023).

10 Cal. Code Regs. tit. 11, § 7004(b) (2023) (proposed).

11 See Col. Rev. Stat. § 6-1-1303(9) (2023).

12 See Conn. Gen. Sta. § 42-515(11) (2023) ("'Dark pattern'... includes, but is not limited to, any practice the Federal Trade Commission refers to as a 'dark pattern.'").

telecommunications provider or a video game designer and see how it applies to your business. While Vonage and Epic Games are dramatically different companies, the practices at issue are common in any business that interacts with consumers. Both companies struggled with presenting consumer choice, and both companies did not mirror their enrollment and cancellation processes. By examining the FTC's complaints in *Vonage* and in *Epic Games*, it becomes apparent that the throughlines in the FTC's enforcement are not industry-specific and can, in fact, serve as a touchstone for any business that interacts with consumers.

A. Analyzing Vonage

Vonage markets Voice over Internet Protocol ("VoIP") phone services products to residential and business consumers. Prices for Vonage's service range from $4.99 to over $50 a month.[13] Vonage offers a variety of enrollment methods, including a 24/7 website or through a toll-free telephone number.[14] However, the cancellation process is more difficult to navigate than the enrollment process. Between 2017 and 2022, Vonage only allowed customers to cancel their enrollment by speaking with a live "retention" agent over the phone.[15] Vonage did not present this requirement to consumers when they enrolled in Vonage's services; rather, it was buried in a lengthy terms of service document.[16] Even finding the telephone number for reaching the retention agents was a hurdle for consumers; while Vonage prominently displayed its main customer service telephone number on its website, the special cancellation number was not presented to consumers in an immediately obvious manner.[17]

For customers whose plans were billed at less than $60 a month, the cancellation process was even more obtuse: first, they had to request a cancellation via online chat and wait to be connected with a live chat agent; then, the live chat agent would have to transfer their call to a live retention agent, requiring an additional wait.[18] Additionally, Vonage put in place "Early Termination Fees" for customers who wanted to cancel before the end of their contract period–but did not conspicuously disclose these terms.[19] Vonage presented the disclosure in a small, unbolded font against a gray background, in contrast to the bolded, larger font disclosing the benefits of signing up for Vonage.[20] For customers signing up over the phone, Vonage instructed its employees to not "proactively" offer information about the Early Termination Fees.[21]

> ***"Vonage markets Voice over Internet Protocol ("VoIP") phone services products to residential and business consumers***

There are two key things to note about Vonage's business practices that resulted in the FTC action. First, their consumer choice presentations were not accurate. Material information was obscured in such a way that only a particularly vigilant consumer would be aware of it. The average consumer would not find an accurate disclosure for the service they were signing up for. Likewise, the "consumer journey" (the process a consumer takes to consent to enroll in a service, and the process taken to revoke that consent) to cancel their Vonage account was circuitous and frustrating, designed more to ensure customers continued to pay for a Vonage account instead of allowing them to cancel their membership at their will.

Vonage eventually agreed to a $100 million settlement with the FTC.[22] While Vonage is a cloud telecommunications service and Epic Games is a video game designer, many of the problems Vonage encountered were similar to the

13 See Compl., *Fed. Trade Comm'n v. Vonage Holdings Corp.*, Case No. 3:22-cv-6435, ECF No. 1 (D.N.J. Nov. 3, 2022).

14 *Id.* at 5-6.

15 *Id.* at 6.

16 *Id.* at 7.

17 *Id.* at 7-8.

18 *Id.* at 9.

19 *Id.* at 11-12.

20 *Id.*

21 *Id.*

22 Press Release, Federal Trade Commission, FTC Action Against Vonage Results in $100 Million to Customers Trapped by Illegal Dark Patterns and Junk Fees When Trying to Cancel Service (Nov. 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.

practices the FTC would cite in its complaint against Epic Games.

B. Analyzing Epic Games

Epic Games develops and distributes the video game Fortnite. Part of Fortnite's appeal is that it is free to download and play, although like many games it offers certain in-game benefits that must be purchased with actual money. Fortnite is incredibly popular, with over 400 million players worldwide.[23] For in-game purchases, Epic would save consumers' payment information by default and use it to bill consumers for future charges.[24] Despite this, Epic prominently advertises Fortnite as free; if a consumer were to download Fortnite on a personal computer, they would only find a small disclosure stating "In-Game Purchases" at the very bottom of the download page.[25]

Once Epic had saved a consumer's credit card information, players – many of them children and teenagers – could make in-app purchases "simply by pressing buttons with no parental or card holder action or consent."[26] There were no safeguards to prevent children from making purchases without parental consent – much to the surprise of parents reviewing their credit card bills.[27] Epic knew this, and internal documentation noted that "Unrecognized and Fraudulent Charges" was among the top five reasons customers complained to Epic Games.[28] In response to these complaints, Epic gave consumers the option not to have their credit card information saved – but only in a small checkbox in the checkout page, with a small print notice to "[m]ake this a one-time payment."[29] Indeed, Epic never informed consumers that the default option was to automatically bill saved credit card information, and it was aware consumers typically did not check the small checkbox.[30]

The in-game purchase flow for Fortnite was also designed in such a way that it was easy for consumers (particularly children) to make accidental or unwanted purchases. For example, in the "Cosmetics" store (where players could preview popular costume changes for their in-game avatars), Epic would automatically charge consumers if they pressed a certain button, without requiring any further action from consumers, such as asking them to confirm their purchase.[31] In contrast, players wishing to cancel an unwanted purchase had to press *and hold* the button in addition to confirming their request for a refund.[32]

> ***Epic Games develops and distributes the video game Fortnite***

Epic did not even offer an option to cancel certain charges until June 2019. Initially, the "Undo" option was presented in a visually identical manner as the purchase option.[33] However, Epic soon reduced its prominence, changing its name to "Cancel Purchase," reducing its size, moving it to the bottom of the screen (away from the "Purchase" button), and requiring consumers to push and hold a button to cancel.[34] Once these changes were made, Epic "observed a roughly 35% decline" in the number of consumers undoing their purchases.[35]

Even requesting refunds was a convoluted process compared to the simple purchase procedures. To find the link to request a refund, consumers had to go to a "Settings"

23 See Natasha Singer, *Epic Games to Pay $520 Million Over Children's Privacy and Trickery Charges*, N.Y. Times (Dec. 19, 2022), https://www.nytimes.com/2022/12/19/business/ftc-epic-games-settlement.html.

24 See *In re Epic Games, Inc.*, F.T.C. File No. 192-3203 (Dec. 19, 2022) at 2.

25 *Id.* at 3.

26 *Id.* at 4.

27 *Id.*

28 *Id.*

29 *Id.* at 5.

30 *Id.*

31 *Id.* at 7.

32 *Id.*

33 *Id.* at 10.

34 *Id.*

35 *Id.* at 11.

tab on the Fortnite app menu, "far removed from the purchase screen," despite the fact that requesting a refund is not a game or device setting.[36] The designer even admitted that he put the link there in an "attempt to obfuscate the existence of the feature" and "add[ing] friction for friction's sake."[37]

Epic deliberately advertised its product as free, and then concealed the nature of its in-game purchase policies. It made the purchase process frictionless but went out of its way to make the refund process cumbersome. By hiding the nature of its in-game purchase policies, Epic tricked consumers into making choices they might not have otherwise made by saving their credit cards. By making its refund process burdensome–with the stated goal of curtailing user refund requests–it was preventing consumers from revoking their consent. Epic Games wound up settling with the FTC for $245 million.[38] Epic was aware that its policies were hindering consumer choice, but rather than addressing these consumer hurdles, they doubled down and wound up paying a substantial fine for it.

02
DEVELOPING BEST PRACTICES

By analyzing *Vonage* and *Epic Games*, certain commonalities in enforcement emerge, allowing us to begin to define what a dark pattern is. The way material information is presented – or hidden – is relevant in the FTC's analysis. Likewise, the consumer journey – the process a consumer takes to consent to enroll in a service, and the process taken to revoke that consent – is closely scrutinized. To borrow a phrase from the Epic Games engineer, "friction for friction's sake" is highly suspect. These general best practices were derived from an analysis of enforcement actions the FTC has taken over the last decade, up to and including *Vonage* and *Epic Games*. They can be divided into two categories: Considerations for Robust User Notice and Choice, and Considerations for User Interface Design.

A. Considerations for Robust User Notice and Choice

When determining how to present consumers with notice and choice, the three topline concerns for any business looking to avoid dark patterns should be accurate disclosures, seamless revocation processes, and the use of straightforward language.

1. Accuracy

In order for a disclosure to be accurate, all material terms and conditions should be included when obtaining consumer consent. Terms and conditions should be stated in an easy to understand way that is unlikely to deceive consumers.[39] In particular, a business should avoid employing "negative options," provisions "under which the customer's silence or failure to take affirmative action to reject goods or services or to cancel the agreement is interpreted" as consent.[40] Businesses should also avoid telling consumers their data is needed for a service to operate when in actuality it is not.[41]

The FTC has been clear about this need for accuracy for many years. For example, in 2015, the FTC brought an action against PaymentsMD, LLC, a medical billing provider, alleging the company failed to inform consumers that it would be collecting sensitive health information from third parties.[42] In 2018, the FTC sued PayPal, Inc., over disclosures in its mobile payment app Venmo.[43] The FTC alleged that PayPal failed to provide conspicuous disclosures of material terms to consumers when first signing up for the app, in violation of the Gramm-Leach-Bliley Act and subsequent FTC regulations.[44] And in 2019, the FTC sued Office Depot, Inc., in a case alleging that a service Office Depot advertised as a free PC checkup program was actually a

36 *Id.*

37 *Id.*

38 Press Release, Federal Trade Commission, Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges (Dec. 19, 2022) (https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations).

39 See, e.g. *In re PayPal, Inc.*, F.T.C. File No. 162 3102 (May 23, 2018); *In re PaymentsMD, LLC*, F.T.C. File No. 132 3088 (Jan. 27, 2015).

40 Telemarketing Sales Rule, 16 C.F.R. § 310.2(w) (2023).

41 See Compl., *Fed. Trade Comm'n v. Office Depot, Inc.*, No. 9:19-cv-80431, ECF No. 1 (S.D. Fla. Mar. 27, 2019).

42 See *PaymentsMD, LLC*, F.T.C. File No. 132 3088 at 2.

43 See *PayPal, Inc.*, F.T.C. File No. 162 3102 at 11.

44 *Id.*

tool to sell diagnostic and repair services to unsuspecting consumers.[45]

The subversion of consumer choice in these examples is plain. When a consumer is not given all the material information, they need to make a decision – whether it is a decision to opt out of tailored advertising, to download an app, or to sign up for a service–the consumer's consent is not informed. When disclosures are not conspicuous, or hidden away on other parts of a platform, an unknowing consumer could reasonably determine they have been given all the material information they need to make a decision. Likewise, when a disclosure is dishonest about what a consumer needs to know, especially when there is a cost (monetary or otherwise) the consumer must pay when they make their decision, it could influence the consumer's choice in an unlawful way.

2. Seamless Revocation

The revocation of consent can take several forms, including canceling a purchase, unsubscribing, or opting out. The revocation process should be seamless; that is, it should be easy for a consumer to do while also providing the consumer with complete information about the revocation process.[46] The number of steps in the "consumer journey" to revoke consent (i.e. the discrete actions a consumer must take) should be equal to the consumer journey to sign up for a service.[47]

Providing all material information is critical. In 2016, the FTC reached a settlement with NutraClick, a company that sold nutritional supplements and beauty products, over its cancellation practices.[48] NutraClick enrolled consumers into a recurring monthly program when they ordered a "free trial" of NutraClick's products, and failed to disclose the enrollment.[49] After settling with the FTC, NutraClick continued to employ dark patterns in its business practices by failing to conspicuously disclose that consumers must cancel their free trial at least one day before the end of the trial period, or else they would be automatically charged for enrollment.[50]

"The revocation of consent can take several forms, including canceling a purchase, unsubscribing, or opting out

In 2020, the FTC sued Age of Learning, Inc., which operated the online children's education platform ABCmouse.com. On the signup page for ABCmouse.com, Age of Learning represented that it had "Easy Cancellation" (in bold, red text) promising that consumers could "cancel at any time."[51] Enrollment in ABCmouse.com could be done on one page with a single form.[52] Cancellation, however, was a more circuitous process. Consumers could not cancel by telephone, email, or by web form, like they could for signing up. Instead, they had to go through four separate pages of ABCmouse.com for a link labeled "Cancellation Policy," which in actuality was the cancellation mechanism.[53]

By making the revocation process onerous, the offending companies were effectively trapping consumers into continuing to pay for services they did not want to receive. The longer the consumer journey was, the less likely consumers were to actually revoke their consent. Even before the enactment of laws specifically prohibiting the use of dark patterns, the FTC was able to enforce against these practices with its authority under the FTC Act.

3. Straightforward Language

Notice presented to a consumer should be as clear and straightforward as possible. As a matter of California law, businesses cannot use double negatives (e.g. "Don't not sell my personal information"), nor can they require consumers to click through or listen to a list of reasons for why they should not revoke their consent.[54] In the *Age of Learning* enforcement matter, the FTC noted that ABCmouse.com also

45 See Compl., *Office Depot*, No. 9:19-cv-80431, at 2.

46 See Compl., *Fed. Trade Comm'n v. NutraClick, LLC*, No. 2:20-cv-08612, ECF No. 1 (C.D. Cal. Sept. 21, 2020) (*NutraClick* II).

47 See Compl., *Fed. Trade Comm'n v. Age of Learning, Inc.*, No. 2:20-cv-7996, ECF No. 1 (C.D. Cal. Sept. 1, 2020).

48 See Compl., *Fed. Trade Comm'n v. NutraClick, LLC*, No. 2:16-cv-06819, ECF No. 1 (C.D. Cal. Sept. 12, 2016) (*NutraClick* I).

49 *Id.* at 3.

50 See *NutraClick* II at 5.

51 Compl., *Fed. Trade Comm'n v. Age of Learning, Inc.*, No. 2:20-cv-7996, ECF No. 1 (C.D. Cal. Sept. 1, 2020).

52 *Id.* at 6.

53 *Id.* at 11.

54 Cal. Code Regs. tit. 11, § 999.315(h)(2)-(3) (2023).

required consumers to scroll through a list of reasons why they should not cancel their membership, including a list of ways to "upgrade" their membership.[55] While businesses have a First Amendment right to inform consumers about the products they offer or the services they provide, it is important to deploy neutral language that does not pressure consumers into making a particular choice.

For companies that rely on technologies such as cookies to remember user settings, these settings can be reset when a consumer clears their cookies or they expire, or they are browsing on a new, unrecognized device or from a different IP address. In these instances, companies should be aware of this situation and should notify consumers and provide them with the opportunity to reestablish their privacy settings.

By using straightforward, concise language, a business interacting with a consumer can ensure that it has provided all material information necessary for a consumer to make an informed choice.

B. Considerations for User Interface Designs

In designing the user interfaces for consumer choice mechanisms, many of the considerations that businesses must take in presenting consumer choice are present. Businesses should avoid using unnecessarily confusing language, and they should avoid an overly long consumer journey. They should also ensure that in consumer interactions actually present a choice and do not infer one; for example, in a banner notifying consumer that a website uses cookies to collect information for personalized advertisements, the banner should have an "Accept" and "Deny" button as opposed to just an "Accept" button, or indeed, no button at all, just a means of closing the banner.

In 2019, the FTC brought an action against AH Media Group, a company that sold personal care and dietary supplements online. In its complaint against AH Media, the FTC noted AH Media's relevant terms and conditions for free trial offers were often obscured on their websites, using small, hard to read fonts that blended in with the background color of the website.[56]

When presenting any notice to consumers, businesses should ensure that the text is legible on both desktop and mobile devices, and that instructions for revoking consent are not hidden in a place consumers would not think to look. If the goal is to avoid dark patterns, the business should state all material terms in a single, easy to find location, displayed in a visually neutral manner.

03
CONCLUSION

The practices the FTC cited in its complaint against Epic Games are nearly identical to the practices the FTC cited in its complaint against Vonage. They are practicing the FTC has cited in complaints against a variety of businesses over the last decade, practices that cut across industry. They are practices that any business that interacts with consumers – whether it's an ad tech company collecting consumer data online or the manufacturer of personal hygiene products marketing a monthly subscription service – must bear in mind.

The FTC has begun to name dark patterns for what they are, but in many ways this is just giving old enforcement practices a rebrand. By specifically calling these practices dark patterns, the FTC is making its priorities plain. As the FTC continues to enforce against dark patterns, buttressed by state attorneys general with specific authority over the use of dark patterns, companies should ensure their interactions with consumers and the design choices they make are straightforward and neutral. ■

"In designing the user interfaces for consumer choice mechanisms, many of the considerations that businesses must take in presenting consumer choice are present

55 See Compl., *Age of Learning, Inc.*, No. 2:20-cv-7996 at 14.

56 See First Am. Compl., *Fed. Trade Comm'n v. AH Media Group, LLC*, No. 19-cv-04022-JD, ECF No. 74 (N.D. Cal. Oct. 23, 2019) at 14.

DARK PATTERNS: PROTECTING CONSUMERS WITHOUT HINDERING INNOVATION

BY
VICTORIA DE POSSON

Victoria is the Secretary General of the European Tech Alliance ("EUTA") which gathers major European digital champions and scaleups successfully built across Europe. The EUTA aims to develop smart policies promoting European tech innovation, investments, and competitiveness. See https://eutechalliance.eu.

01 INTRODUCTION

Practices such as pop-ups offering "free prizes," false countdown timers promoting special deals, and automatic billing after a free trial without prior notification do not only manipulate users, but also significantly deteriorate their online experience. Many businesses already avoid such misleading or unfair commercial practices, in line with prohibitions under legislation. Nevertheless, in the policy debate these practices are resurfacing under a new label: "dark patterns."

This article aims to examine in more detail the concept of "dark patterns" and the necessity for their regulation. It will begin by exploring the origin and definition of the term, comparing online and offline techniques, and evaluating

the need for flexible design interface rules. Finally, this article will take a closer look at the regulations in the European Union ("EU"), as it is widely recognized as a global leader in regulating the online sphere and protecting consumers.

02

DARK PATTERNS: ORIGIN AND DEFINITION OF THE TERM

As politicians seek to ban "dark patterns," it is crucial to establish a clear definition of what constitutes a "dark pattern." This will ensure that consumers are safeguarded against misleading practices while simultaneously avoiding any hindrance to the development of intuitive and user-friendly interfaces that serve legitimate purposes.

The terminology of "dark patterns" was first coined in 2010 by English user experience specialist Dr. Harry Brignull, who holds a PhD in Cognitive Science. Brignull defines "dark patterns" as "*tricks used in websites and apps that make you do things that you didn't mean to*."[2]

When it comes to defining the concept of "dark patterns," the challenge is to identify the line that separates legitimate user interface design from deceptive practices. Over the last few years, the use of the "dark patterns" term is moving further and further away from Brignull's initial definition. It has become a catch-all term encompassing commercial practices that include some legitimate business marketing practices.

For instance, the pressure to ban consumer reminders of their previous choices through interfaces, which can be a valid and well-intentioned practice. The choices presented can vary based on the time and context, reflecting different use cases and intentions. Users should have the ability to revisit their choices when there is a clear demand or user interest. This could include situations where users are asked to review their privacy settings periodically.[3]

"Dark patterns" would be better defined as design choices that intentionally distort the behavior of the average user for manipulative purposes. Prohibitions should not target practices that are made in good faith and have a legitimate purpose or are justified in specific situations. For example, requests for location access to improve user preferences or awareness tools that enhance safety and privacy should be allowed.

Measures must be limited to "dark patterns" that are illegitimate in any scenario and tackle the issue comprehensively across the internet. Given the inherent vagueness of the concept and its lack of legal foundation, it is crucial to have clear guidance based on robust research on what might constitute a dark pattern. Sufficient flexibility should be left for a case-by-case assessment of the real impact and intention behind a practice.

03

DARK PATTERNS: ONLINE AND OFFLINE MARKETING TECHNIQUES

An outdated perception is that online businesses and platforms are often associated with a tendency to manipulate customers. This view stems from an inaccurate belief that the digital world is still unregulated and chaotic and is more representative of when the internet emerged rather than where it is today. Despite the significant increase in regulatory texts on online practices in recent years, with the motto "what is forbidden offline must be forbidden online," remnants of this fear of the digital world are still evident. This perception highly penalizes online businesses compared to brick-and-mortar ones, in particular when it comes to the ambiguous notion of "dark patterns." Indeed, the desire to create additional regulation marks a turning point as marketing practices that are legal offline are becoming illegal online.

Visual merchandising in physical marketing in the offline world is the equivalent to website design marketing in the online world. It involves strategically presenting, arranging, and displaying merchandise in stores to attract customers and boost sales. This concept was initially introduced in the retail industry in 1883 by Harry Gordon Selfridge, an American entrepreneur who established Selfridges, a London-based department store.[4]

2 Harry Brignull, *What are deceptive patterns?,* April 14, 2023, accessible at: https://www.deceptive.design/.

3 Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, November 29, 2017, accessible at: https://ec.europa.eu/newsroom/article29/redirection/document/51025.

4 Johnson & Wales University, How Visual Merchandising Serves as Marketing: Understanding the Impact Across Industries, April 12, 2023, accessible at: https://online.jwu.edu/blog/how-visual-merchandising-serves-marketing-understanding-impact-across-industries.

Some of the practices that are called out for being "dark patterns" are actually visual merchandising techniques used by brick-and-mortar retail. For example, interface designs that highlight or lowlight certain information or sections of a website correspond to visual techniques used by stores when displaying products. The choice of the location of products on a shelf, or the location of the shelf itself in a store is purely strategic marketing. The display of popular products at the bottom or at the top of a shelf instead of at eye level has never been called out for being a "hidden in plain sight" deceptive commercial practice.[5] The same goes for the de-emphasis of a product displayed with multiple other products on a shelf, which has never been considered a "too many options" deceptive practice.[6] The way a product is displayed and emphasized or not, based on factors such as its location, the use of color contrasts, or neon lighting, is a legitimate marketing technique in physical retail.

Another example would be an interface with messages pointing out limited time for a promotion, countdowns, or information on stock and quantity. The same type of messages can be found on the windows of stores. Words, colors, and illustrations are strategically used to encourage passers-by to enter shops. The same goes for messages on ongoing or soon-to-end promotions strategically displayed inside the store on shelves and walls, or even orally announced to customers.

Where these are legitimate, these visual commercial techniques are accepted for physical retail and the same should stand for the digital world. Online persuasive design practices should be distinguished from deceptive ones in order to ensure the same commercial rights to online businesses as to brick-and-mortar ones but also to ensure the best online user experience.

04

DARK PATTERNS: NEED FOR FLEXIBLE DESIGN INTERFACE RULES

It is evident that practices that deceive or mistreat consumers should be prohibited. Regulators should not take the easy way out by standardizing online interfaces. Instead they should enable the best consumer experience online and foster a competitive and innovative environment for businesses incentivizing creativity.

Differentiation of online interfaces and visual elements is crucial for businesses to establish their brand identity and for users to identify and distinguish between brands. This distinction is vital for business success and optimal user experience. Implementing a standardized approach could limit freedom of enterprise and innovation, creating a homogenous online landscape.

A standardized interface would also be detrimental to the consumer experience, as a one-size-fits-all approach would not work for most services, particularly emerging ones. For instance, for some services it makes sense to have a consumer support access on their homepage, while for other services it should be under a separate page, like a support page, as their home page is intentionally minimalist to benefit consumers' experience. Regulators must keep a flexible approach that takes into account the variety of online business models and allows businesses to implement rules that make sense for their services and products. Otherwise, their well-intentioned efforts may be counterproductive and harm the customer journey on the website, undermining the overall customer experience.

To protect entrepreneurship and ensure the best user experience, regulations on interface design need to offer flexibility, adaptability, and follow a case-by-case approach.

05

DARK PATTERNS: FOCUS ON THE EUROPEAN UNION

A. The Web of EU Rules

Let's examine the regulations on "dark patterns" in the European Union ("EU"), the world's leader in regulating the online world and protecting consumers. Various EU initiatives, including the 2005 Directive on Unfair Commercial Practices ("UCPD"), the 2011 Directive on Consumers Rights, and the 2016 Regulation on General Data Protection ("GDPR"),

5 European Data Protection Board, *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*, March 14, 2022, p. 66, accessible at: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf.

6 *Op. cit*. p. 67.

cover the concept of "dark pattern" techniques by referring to misleading and unfair commercial practices.[7]

The term "dark patterns" was first introduced in an EU text in a study titled "Behavioral study on unfair commercial practices in the digital environment, Dark patterns and manipulative personalization," conducted by the EU Directorate-General for Justice and Consumers in 2016.[8] The report defined "dark patterns" as *"a concept that is generally used to refer to practices in digital interfaces that steer, deceive, coerce, or manipulate consumers into making choices that often are not in their best interests."*[9] This report sparked the interest of European regulators in "dark patterns."

The EU further protects its consumers from deceptive practices by updating its legislative framework including the 2019 Directive on better enforcement and modernization of Union consumer protection rules (also known as the "Omnibus Directive") and the 2021 Guidance on unfair business-to-consumer commercial practices in the internal market.[10]

The recently adopted Digital Services Act ("DSA") is the first EU regulation to define the term "dark patterns." It describes it as "*practices on online interfaces of online platforms that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions*."[11]

The term "dark patterns" has also been introduced into ongoing legislative proposals, such as the General Product Safety Regulation ("GPSR"), the Empowering Consumers for the Green Transition Directive, and the Distance Marketing and Financial Services Directive. [12]

Recently, the European Commission launched a Fitness Check of EU consumer law on digital fairness to evaluate existing regulations and their adequacy for ensuring a high level of online consumer protection.[13] This initiative could lead to new rules on "dark patterns."

However, before considering new EU consumer legislation, policymakers should assess the consistency of the Omnibus Directive, which has only been implemented since May 2022, and other EU consumer protection measures enforced across the EU Single Market. Sufficient time should be allowed for the rules to produce their intended effects before once more amending the rulebook.

> ***"The recently adopted Digital Services Act ("DSA") is the first EU regulation to define the term "dark patterns."***

Instead of introducing new provisions for "dark patterns," clarifying guidelines would be a reasonable next step, as outlined in the DSA, to ensure alignment, coherence, and consistency between existing and future legislation. This is particularly important due to the multitude of digital business models and sector-specific requirements. It is also crucial to prevent any overlap or inconsistency in the regulations that could create legal uncertainty for businesses and consumers.

B. Enforcement

The real problem with unfair commercial practices is not the lack of sufficient regulation, but the enforcement of existing rules. In Europe, enforcement should equally target all com-

7 EU Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market ('Unfair Commercial Practices Directive') (2005), Official Journal L 149, p. 22–39; EU Directive 2011/83/EU on consumer rights (2011), Official Journal L 304, p. 64–88; EU Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (2016), L 119, p. 1–88

8 European Commission, *Behavioural study on unfair commercial practices in the digital environment Dark patterns and manipulative personalisation: final report*, April 2022, accessible at: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418.

9 *Op. cit*., p. 20.

10 EU Guidance C/2021/9320 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 (2021), OJ C 526, p. 1–129.; EU Directive (EU) 2019/2161 on the better enforcement and modernisation of Union consumer protection rules (2019), L 328, p. 7–28.

11 EU Regulation 2022/2065 on a Single Market For Digital Services (Digital Services Act) (2022), L 277, p. 1–102.

12 European Commission, Proposal for a Directive concerning financial services contracts concluded at a distance and repealing, COM/2022/204 final; European Commission, Proposal for a Directive empowering consumers for the green transition through better protection against unfair practices and better information, COM/2022/143 final; European Commission, Proposal for a Directive concerning financial services contracts concluded at a distance and repealing Directive 2002/65/EC, COM/2022/204 final.

13 European Commission, *Digital fairness – fitness check on EU consumer law*, April 19, 2023, accessible at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en.

panies interacting with EU consumers, irrespective of their country of origin or their online or offline origin. Selectively enforcing rules on certain players but being less focused on others is detrimental to consumer protection and can also create market distortions. This would be the case, for example, under the new DSA and GPSR obligations for marketplaces which do not apply to extra-EU retailers.

A more harmonized approach to the implementation of consumer protection legislation is also needed to ensure coherent and consistent enforcement of EU rules, given the cross-border operations of businesses. Divergent interpretations and enforcement lead to uneven consumer standards across EU Member States, generating legal uncertainty for businesses and constraining their potential on cross-border trade. Effective collaboration among Member States (e.g. via the Consumer Protection Cooperation Network) can help ensure more uniformity in the interpretation and enforcement of EU rules.

The EU legislator should incentivize Member States' sectoral authorities (e.g. consumer, competition, data protection, and telecommunication authorities) to better cooperate to ensure pro-innovation as well as a coherent and harmonized application of EU rules. A holistic approach at national level should be adopted. In other words, silos and diverging interpretations must be avoided within the same country and among EU Member States.

06
CONCLUSION

"Dark patterns" are design choices intentionally made to manipulate the average user's behavior for deceptive purposes. The term was first coined in 2010 by Harry Brignull, but its definition has since expanded to encompass even some legitimate business marketing practices. The challenge therefore lies in identifying the line that separates legitimate user interface design from deceptive practices, which is why clear examples of "dark patterns" supported by robust research are crucial.

Although online businesses and platforms are often associated with a tendency to manipulate customers, it is important to distinguish online persuasive design practices from deceptive ones to ensure the same commercial rights to online businesses as to brick-and-mortar ones. Measures must be limited to "dark patterns" that are illegitimate in any scenario and tackle the issue comprehensively across the internet.

It is important to avoid taking the easy way out and standardizing online interfaces, as differentiation of online interfaces and visual elements is crucial for businesses to establish their brand identity and for users to identify and distinguish between brands.

In Europe, regular assessment of consumer protection rights is to be welcomed. However, before adding another layer to the already well-equipped *consumer acquis*, EU policymakers should focus on better and more consistent enforcement of existing rules and allow time for these rules to take effect. That said, EU guidance would be welcomed in areas where EU rules overlap and/or conflict, as this would also support a more coherent and uniform interpretation and enforcement of the rules across the EU.

"Dark patterns" are design choices intentionally made to manipulate the average user's behavior for deceptive purposes

DARK PATTERNS AND MANIPULATION

BY
MARCELA MATTIUZZO

PhD Candidate at the University of São Paulo, Visiting Fellow at the Information Society Project at Yale University. Partner in competition law and data protection at VMCA.

As noted by Thaler, Sunstein & Balz,[2] people do not make decisions in a vacuum. Rather, they decide in specific environments. Those who design the environments in which decisions are made are referred to as "choice architects" and have considerable power in influencing what those decisions will be, precisely because they are able to meddle with features of that same environment (Thaler, Sunstein & Baltz 2010).[3] As behavioral science has shown, rather than being fully rational, utility maximizing individuals, human beings are highly susceptible to all kinds of influence. Becoming aware of the susceptibilities of individuals to such influence can allow choice architects to create designs that foster specific decision-making.

2 Thaler, Sunstein & Balz, Choice Architecture (SSRN Electronic Journal, 2010).

3 *Ibid*. 4.

Literature and research on how precisely individuals behave, and how that behavior significantly departs from what would be expected from the *homo economicus*, is vast and far-reaching.[4] By now, three Nobel prizes have been granted to academics that dedicated their careers to behavior studies.[5] The field of behavioral economics has grown and provided relevant information not only to economists, but also to policymakers concerned with devising better strategies and solutions in tackling the incentives for individuals to act in certain ways.

The limits of human rationality (or bounds of human behavior) are relevant not just because they allow for a better description of how individuals act, but also because – and this is of paramount relevance – research has shown that biases are predictable and have patterns (Thaler & Sunstein, 2008). In other words, it is not that behavioral science has destroyed the usefulness of economic models by concluding humans operate in entirely unpredictable ways, but rather that it has shown predictability within irrationality.

As highlighted by Akerlof & Shiller, behavioral economics is relevant not because it shows how human beings are entirely irrational and it is therefore impossible to predict their actions. On the contrary, it is relevant because it allows for better prediction of human behavior, as academics have long been able to identify patterns in irrationality[6] – for example, reasons for procrastination or decision paralysis. For that same reason, behaviorism facilitates rather than impedes economic debates that are essential in drafting norms. If individuals do not respond as rational agents that are always maximizing their own interests, but frequently fail to reach that goal for reasons that repeat themselves over time, then one can (and should) use that information to design legislation that better protects consumers and incentivizes competition.

Likewise, because irrational patterns are predictable, they open room for manipulation – and more specifically for choice architects, if they so wish, to make use of manipulative strategies. Given individuals tend to act in similar ways, and that their actions are not fully rational, one can explore the limits of rationality to steer people towards reaching certain conclusions and acting in certain ways. The goal of this article is to propose a discussion on the (ir)relevance of the concept of manipulation in defining the (un)lawfulness of the use of choice architecture, and more specifically of dark patterns, in online environments.

As highlighted by Akerlof & Shiller, behavioral economics is relevant not because it shows how human beings are entirely irrational and it is therefore impossible to predict their actions

First it is important to clarify that the term "dark pattern" has no ultimate and final definition. In trying to provide an overview of the variety of definitions for dark patterns, Mathur et al. identified 19 instances in which the term was defined. They explain that after Harry Brignull first introduced the term in 2010 on the website darkpatterns.org, describing dark patterns as "tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something," there was a flurry of academic research that made use of the expression (p. 3).[7] Their research has revealed what they understand to be four different "facets" of dark patterns, namely: (i) characteristics of the user interface that can affect users, (ii) the mechanism of effect for influencing users, (iii) the role of the user interface designer, and (iv) the benefits and harms resulting from a user interface design (Mathur, Mayer & Kshirsagar, 2020).[8]

I will provide a more specific definition of how I believe dark patterns can be understood throughout this article, but for now it is enough to say that they are the deployment of choice architecture that influence users' decision-making.

If one deploys choice architecture in the online environment, it is not immediately clear that such conduct should be unlawful. First, for an obvious reason: because the result can be beneficial to the user. For instance, if someone decides to design a platform in a way that allows for the user to be given more information and more accurate details about the products she is about to buy, that is likely to be good for that person. But the issue I am interested in debating regards scenarios in which negative impact to consumers do take place. In that context, it is important to thoroughly examine the idea of manipulation as a specific form of influence, to better understand what about this deployment of choice architecture would be potentially unlawful. Is the mere fact that manipulation is taking place – and users' decision-making being influenced - the issue, or does the problem lie solely when the result of such influence is detrimental to consumers?

4 Richard H. Thaler, From Homo Economicus to Homo Sapiens (Journal of Economic Perspectives, Volume 14, Number 1, 2000).

5 Herbert Simon was awarded the Nobel Prize in Economic Sciences in 1978, followed by Daniel Kahneman and Vernon Smith in 2002, and more recently by Richard H. Thaler, in 2017.

6 Akerlof & Shiller, Phishing for phools: The economics of manipulation and deception. (Princeton University Press, 2015).

7 Marthur, Mayer & Kshirsagar, What Makes a Dark Pattern... Dark?: Design Attributes, Normative Considerations, and Measurement Methods. (Proceedings of the 2021 CHI conference on human factors in computing systems, 2021), 3.

8 *Ibid*.

01
CONCEPTS OF MANIPULATION

To discuss whether manipulation is lawful, we must first debate in more depth what exactly manipulation entails. First and foremost, we should note that there is ample debate on the concept of manipulation and it is by no means straightforward to devise its precise contours.

Jongepier & Klenk contribute to this discussion by asking a question that is of particular relevance here: whether there is anything that makes online manipulation effectively different from offline manipulation (and if so, what is that).[9] They start out by clarifying that the specific characteristics of manipulation as a concept are hard to define, but also that "the study of manipulation does not stand or fall with the propensity of the concept 'manipulation' to bend to complete analysis in terms of necessary and sufficient conditions. Manipulation, though perhaps vague, varied, and beset with borderline cases, may yet be unified by Wittgensteinian family resemblance, that is, not a set of shared properties but a resemblance to paradigm cases of manipulation."[10] In that light, they propose a search for "demarcating factors" that aim at distinguishing manipulation from other practices, carrying out a literature review of recent work in this field. Their conclusion is that it is important to form a theory of manipulation that has clear methodology, and to clarify one's aim in developing such theory (Jongepier & Klenk, 2022).[11]

In that light, it is not the objective of this piece to provide a definitive answer to the question on what manipulation entails, though I do aim at providing a definition useful for the purposes of the dark patterns debate. I adhere to Susser et al.[12] understanding that manipulation is a form of influence which specifically attempts to "change the way someone would behave absent the manipulator's interventions." Manipulation, in that sense, is different from other practices such as persuasion or coercion, because it involves "taking hold of the controls" and to "displace [people] as the deciders."[13] In other words, "whereas persuasion and coercion work by appealing to the target's capacity for conscious decision-making, manipulation attempts to subvert that capacity."[14]

It is important to note that the central aspect of this definition of manipulation emphasizes that to manipulate has nothing to do with leading a person to make non-ideal decisions, as someone can be manipulated into making better decisions. The covertness of manipulation is much more important in its definition than the goal of the manipulator. This is where dark patterns and manipulation differ. Manipulation can be employed "for good" and, in the now famous concept popularized by Thaler & Sunstein, individuals can be "nudged" toward making better decisions, even if that process involves some level of hiddenness.[15] Dark patterns, however, always, and by definition (or at least according to the definition I intend to propose herein) lead individuals to be worse-off.

02
MANIPULATION AND TECHNOLOGY

A second aspect that requires further analysis is whether manipulation is at all different when it is deployed by use of technology. Jongepier & Klenk propose that there are aggravating factors regarding technology that should be taken into consideration, namely: personalization, opacity, flow, and lack of user control.[16] Personalization, understood as "the way in which (e.g. machine learning) algorithms are designed such that they can deliver something that is in line with the user's preferences, personality, and so on" (p.

9 Jongepier, Fleur & Klenk, M. B. O. T. The Philosophy of Online Manipulation. (Routledge - Taylor & Francis Group, 2022).

10 *Ibid*. 17.

11 *Ibid*. 19.

12 Susser, Roessler & Nissenbaum. Online Manipulation: Hidden Influences in a Digital World. (GEORGETOWN LAW TECHNOLOGY REVIEW, 2019).

13 *Ibid*. 16.

14 *Ibid*. 17.

15 A nudge, as Thaler & Sunstein describe, "is any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting the fruit at eye level counts as a nudge. Banning junk food does not." Thaler & Sunstein. Nudge: Improving Decisions About Health, Wealth, and Happiness (Yale University Press, 2008), 6.

16 *Ibid*. 35.

35) has the potential to enhance the relevance and effectiveness of manipulation. The idea of opacity, though itself debatable, relates to lack of transparency. Flow, for its turn, refers to user's seamless online experience – which though overall desirable can "prevent one from being aware of relevant knowledge, can hamper one's opportunities to reflect, can bypass one's rationality, and thus prevents one from gearing one's behavior in directions that better ft one's larger or deeper desires or ideals" (p. 39). Finally, lack of user control means there is little a user can do, even when she is aware that she is trapped inside a filter bubble, to break out.

The observations by Jongepier & Klenck should be understood in light of other authors' contributions. Notably, the idea of market manipulation was first coined by Hanson & Kysar[17] in a famous piece from the 1990s that aimed specifically of making use of behavioral science to show how market outcomes can be influenced. In their words, "[the] susceptibility to manipulation produces an opportunity for exploitation that no profit-maximizing manufacturer can ignore."[18] As the authors very poignantly point out, the possibility of manipulating consumers is relevant because it means firms have no other option than to capitalize on it, otherwise they will be losing precious market opportunity. That gives rise to a market failure: consumer biases are an endogenous force that shapes markets.

The observations by Jongepier & Klenck should be understood in light of other authors' contributions

Calo proposed an adaptation of the concept to current terms by calling Hanson & Kysar's proposal "nudging for profit."[19] He further clarifies that though the idea of manipulation in markets was already relevant back in the 1990s, it became significantly more important once the mediated consumer and big data came about – roughly put, the mediated consumer is one that does not interact directly with firms that provide goods or services, rather purchases *through* devices, leaving a trail that can be used to firms' benefit, precisely to design strategies aimed at manipulating behavior; the use of big data, in turn, involves "parsing very large data sets with powerful and subtle algorithms in an effort to spot patterns."[20] Calo argues that companies can look for biases in these large data sets of consumers' trails and adopt strategies aimed at exploiting vulnerabilities in much more effective ways than before.[21]

Another aspect that deserves a deeper dive in clarifying the relevance of technology is choice architecture – and more specifically the role of architects in shaping decision-making. The concept of choice architecture, as stated previously, has been around for some time. The deployment of this concept in digital markets, just like digital markets themselves, is more recent. It is not particularly challenging to understand that how options are presented to us makes a difference in determining what we effectively choose. But the devil is in the details and the relevance of choice architecture is ever greater the less we are able to easily identify it.

More radical illustrations on the relevance of design can be found in gambling. In Addiction by Design,[22] Schull clarifies that the enterprise that sustains gambling is based on reinforcement schedules. That means gambling machines, such as slot machines, are built in ways that hook the player based on a simple logic of providing rewards for their actions. The trick is that, though on the one hand the person knows that rewards can be awarded, she is entirely unable to predict *when* those rewards will be granted. Referencing the studies by Skinner, the author highlights that those schedules can be stretched by "someone who controls the odds"[23] – or as I would call it, by the choice architect. Schull also highlights that the adjustments made to game development do not simply "detect and conform to existing market preferences, [but rather] have transformative effects on those preferences."[24]

In a similar light, Hartzog identifies the relevance of choice architecture in connection to privacy. The author very adamantly points out that, as much as we are led to believe otherwise,

17 Hanson & Kysar, Taking Behavioralism Seriously: The Problem of Market Manipulation (New York University Law Review, Vol. 74,1999), 632.

18 *Ibid*. 722.

19 Ryan Calo, Digital Market Manipulation, (82 George Washington Law Review 995, 2014), 1001.

20 *Ibid*. 1008.

21 *Ibid*. 1008.

22 Natasha Dow Schüll, Addiction by Design: Machine Gambling in Las Vegas, (Princeton University Press, 2012).

23 Burrhus Frederic Skinner, Beyond Freedom and Dignity, (Pelican Books, 1971), 40.

24 *Ibid*. 111.

design is never neutral, because it always "communicates information and enables (or hinders) activities."[25] It provides signals to people, and as such "helps define our relationships and our risk calculus when dealing with others."[26] It also alters transaction costs, by making tasks easier or harder to accomplish. In the online environment in particular, a lot of effort tends to be spent on facilitating interaction, and it has been proven time and again that slight increases in cost can have relevant impacts.[27] With that background, he highlights that the problem with design and privacy lies primarily in market incentives – there are few that lead companies to invest in less data collection, and the more data collected, the more users are subject to potential harm. He further proposes that adequate regulation should focus on design itself, because "the design of popular technologies is critical to privacy, and the law should take it more seriously."[28]

The more important point here is that though the general idea behind choice architecture remains the same – online environments, just like any other environment, must be designed somehow; items have to be displayed in some order, colors have to be chosen for each segment of a page, and so on, and, just like it happens offline, how such choices are framed can be better or worse for users. The complexity and the importance of this debate is larger because online environments are much easier (and cheaper) to design and to experiment on. Designers can deploy several A/B tests in online platforms that they would be unable to run offline. The level of granularity of design options therefore increases. It is not only a matter of choosing if product 1 or product 2 will be placed first, but also a matter of what color will most engage users, what choice of words will be more appealing, what order of placement will provide better results, and infinite other options.

Looking at choice architecture through the lens of behavioral economics allows us to see how they intertwine, and how design can be used, with the help of behavioral biases, to negatively impact both users and markets. As Akerlof & Shiller point out, we must be aware that economic agents will always take advantage of situations in which they can turn higher profits. If they identify behavioral biases that would allow for business opportunity, they will explore such biases. The authors further clarify how this has been done time and time again, in situations as different as the 2008 financial crisis and the pharmaceutical industry.[29]

There is no reason to believe this will be any different in digital markets – in fact there is ample evidence that the same will likely happen to a worse degree. Studies have shown how platforms can deploy choice architecture in ways that may harm either users, markets, or both – notably, the reports on the topic by the UK Competition and Markets Authority ("CMA"),[30] the Organization for Economic Cooperation and Development ("OECD"), and the European Commission ("EC") compile evidence that classifies different methods by which such results may be reached. [31] The OECD also provides some potential explanations on why the deployment of deceptive practices in online environments tend to be more damaging to consumers. They claim that businesses are more aware of opportunities for exploiting behavioral biases, but also that consumers' behavior online is significantly different. They are less attentive, process information less well, more frequently default to simple rules of thumb, and in general are more task-oriented – which consequently allows them to ignore content more easily, as well as underestimate manipulation.[32]

03

THE (UN)LAWFULNESS OF MANIPULATION AND DARK PATTERNS

By adhering to a definition of manipulation that requires a subversion of an individual's capacity to understand what is going on, I suggest that manipulation necessarily involves diminishing people's capacity for rational deliberation. As stated in the previous section, there is reason to believe that the potential to do so in online environments is heightened. The question that can be further discussed, in this

25 Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies, (Harvard University Press, 2018), 26.

26 *Ibid*. 27.

27 *Ibid*. 29.

28 *Ibid*. 7.

29 *Ibid*. 38.

30 See https://www.gov.uk/government/publications/online-choice-architecture-how-digital-design-can-harm-competition-and-consumers.

31 See Behavioural study on unfair commercial practices in the digital environment - Publications Office of the EU (europa.eu), available at https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en.

32 OECD,. Dark commercial patterns. (OECD Digital Economy Papers, No. 336, 2022).

context, is whether manipulation is itself "bad" or, put differently, if individuals who are subject to manipulation have any normative reasons to object to its deployment, even if no concrete decisions that they may have taken while being manipulated result in harm or any unfavorable results.

In attempting to tackle that question, Sunstein notes that manipulation can be considered a moral wrong under both Kantian and welfarist approaches. For Kantians, it is wrong because "it is not respectful of choosers"[33] (p. 1960), offending their autonomy. For welfarists, the risk of manipulation is that it can promote the manipulator's own interest, "rather than those of the chooser" (p. 1961). Furthermore, even when manipulators are acting in the chooser's best interest, they often lack the knowledge of what is best for each chooser, and the results can be equally problematic.[34]

Sunstein also states that though we should be able to agree, on different grounds, that there is a certain category of actions that can be classified as manipulation and that can be harmful to individuals, it might as well be that this category is "properly promoted or discouraged by social norms, but properly unaccompanied by law or regulation."[35] In other words, manipulation may be wrong, but not necessarily illegal. For this reason, he proposes that the best way to counter manipulation is to focus on specific forms of manipulative behavior that are clearly harmful and hard to defend. He suggests that assessing transparency – to what extent people aware of what is going on and of what they are being led to do – and the general goal of the practice *vis-à-vis* the interest of most people subject to it, would be a way forward.[36] Other authors follow similar paths and argue, for example, that the unlawfulness of manipulation should be assessed based on what the manipulator is trying to accomplish.[37]

Instead of trying to provide a general account on how manipulation can be illegal, I will attempt to answer the question on whether manipulation is lawful within the narrow terms of my definition of the concept, as well as within the purposes of the "dark patterns" discussion. To do so, a clearer definition of dark patterns is a helpful step forward. In that sense, I propose that dark patterns must (i) encompass the deployment of choice architecture in the online environment (ii) that manipulates individuals (iii) into achieving a result that is beneficial to the choice architect (iv) and detrimental to the user. In behavioral lingo, dark patterns work by exploring System 1 decision-making while eliminating (or substantially minimizing) System 2 processes.[38]

> ***In attempting to tackle that question, Sunstein notes that manipulation can be considered a moral wrong under both Kantian and welfarist approaches***

In that context, though I believe arguing manipulation is unlawful is viable, I also understand it is not possible to say all forms of manipulation are illegal – for, as mentioned, manipulation can be employed in the manipulee's best interest. Though one could say that the mere subversion of rational capacity for deliberation is a moral wrong, arguing it is legally impermissible is quite different and, in the present context, a burdensome effort that provides minimal practical impact. Given my concept of dark patterns already entails a detrimental result to users, a more functional approach suggests focusing on those impacts instead of devising a theory on the rightfulness of manipulation. Again, that is not to say this is not relevant, nor that it cannot be done, but simply to highlight that a debate on dark patterns need not be constrained to that discussion.

Note that the proposed definition leaves aside yet another aspect that is often part of the debate, that is, whether dark patterns need to encompass *intent* in order to effectively be considered "dark."[39] Devising intent is extremely chal-

33 Cass R. Sunstein, Manipulation as theft. (Journal of European Public Policy, 29:12, 1959-1969, 2022), 8.

34 Sunstein further argues that the welfarist argument is largely based on John Stuart Mill's harm principle.

35 *Ibid*. 1963.

36 *Ibid*. 1964.

37 For example, Eric Posner argues that the end of manipulation "is typically one's own advantage, but it need not be. Parents frequently manipulate their children for the children's interest, and not for (or not just for) the parents'." Eric A. Posner, The Law, Economics, and Psychology of Manipulation. (Coase-Sandor Working Paper Series in Law and Economics No. 726, 2015), 2. .

38 According to Daniel Kahneman, on Thinking, Fast and Slow, "The automatic operations of System 1 generate surprisingly complex patterns of ideas, but only the slower System 2 can construct thoughts in an orderly series of steps."

39 There are two ways intentionality can be understood in this context, according to Jongepier & Klenk: the general intentionality requirement speaks to the requirement that manipulators be agents. The specific intentionality requirement, for its turn, requires "intentions with a particular content" (p. 22). I am here focused on the specific requirement, by which one would need to assess the particular goals of that concrete action.

lenging and, more importantly, often extremely hard to assess, especially when dealing with corporations instead of individuals. And it is precisely because the discussion I aim to carry out is focused on institutions that I suggest leaving aside the debate on whether the goal of the company was indeed to impair individuals' deliberative capacities. Most legislation that deals with corporate conduct understands that whether or not the goal of the company was to reach a given result is relevant in determining sanctions or damage liability, but not central in verifying if the practice was illicit and/or should be penalized. Another reason for leaving that discussion aside is that, as clarified, choice architecture is not accidental or neutral. As such, the way any environment is designed will invariably tend to serve its architects' purposes. Even if the person (or company) in charge did not necessarily anticipate the negative consequences of their choices, the more likely scenario is that the choices themselves are not random. Therefore, it makes sense to assume, at least at first sight, that intent is not an aspect that should be assessed in much detail to establish liability in this context.

If the legality of dark patterns should be assessed not owing to how users were influenced into reaching certain decisions, but rather by focusing on whether those decisions are detrimental or harmful, the focus of the dark patterns debate naturally shifts towards specific practices and their impacts. Lawfulness will be determined by the result of a given conduct, and not by the wrongfulness of the conduct itself.

As I understand it, this approach is significantly simpler and only marginally less useful in terms of policy debates. Again, that is not to say that discussing the legality of manipulation is not relevant, but merely that current research indicates that because this is not a well-defined and uncontroversial concept, assessing whether its deployment is somehow unlawful is not clear-cut and will be context-dependent. In that sense, focusing on effects is a useful shortcut. It serves to show that if manipulation is deployed by use of choice architecture in online environments and the result of that interaction is positive for the company while consumers are negatively impacted, then there is room to deepen the assessment on the lawfulness of the conduct.[40]

As I understand it, this approach is significantly simpler and only marginally less useful in terms of policy debates

40 The specific requirements for legality will then vary depending on what kind of wrongdoing one is interested in assessing. For antitrust, conduct would fall within the rule of reason analysis, and aspects such as market power would have to be investigated. For data protection, issues such as transparency and users' consent might be the most pressing. And so on.

UNCLOAKING DARK PATTERNS: IDENTIFYING, AVOIDING, AND MINIMIZING LEGAL RISK

BY KYLE R. DULL

& JULIA B. JACOBSON

Kyle R. Dull is a senior associate in the Data Privacy, Cybersecurity & Digital Assets Practice at Squire Patton Boggs (US) LLP. He previously served as an Assistant Attorney General prosecuting consumer protection and privacy related offenses. Julia B. Jacobson is a partner in the Data Privacy, Cybersecurity & Digital Assets Practice at Squire Patton Boggs (US) LLP.

Dark patterns are misleading and manipulative design choices intended to influence a consumer's behavior and prevent them from making fully informed decisions about their data and purchases. Dark patterns go beyond clever marketing gimmicks and instead cause users to unwittingly take action against their personal preferences, such as signing up for services they do not want, purchasing products they do not intend to purchase, or surrendering their personal information.

Dark patterns are highly effective at influencing consumer behavior, particularly with less sophisticated users and when layered together. In a recent enforcement action,[2] dark patterns in gaming apps resulted in unauthorized charges because, where a button to advance to the next level is placed immediately proximate to a "buy" button, which automatically generated charges when accidentally bumped or an app advertised as "free" had hidden charges described as qualifiers in fine print placed far from the term "free." These practices caused unaware players to rack up charges, ranging from a dollar to hundreds of dollars, frequently on their parents' credit cards, from the use of a single app or website. While dark patterns are most commonly used in online settings, they also are found in physical stores, and across industries.

Although the term "dark patterns" was coined over a decade ago by Harry Brignull,[3] recently, the consequences of dark patterns have recently received increased consumer protection and privacy regulatory and legislative attention in the United States, EU, and UK.

01
TYPES OF DARK PATTERNS

Dark patterns can be difficult to spot but some of the most commonly used forms include:

· ***Misdirection***: A business uses distracting language or visuals such that users do not fully understand to what they are agreeing. The user interface's design focuses a user's attention on one thing in order to distract the user's attention from another element.
· ***Bait and Switch***: A business offers a product or service at a low price, but then makes the actual purchase process especially complex. A user thinks that their action will have a specific outcome, but in the end, it does not materialize. For example, a business might require users to create an account or enter credit card information before the final price is presented.
· ***Nudging***: A business uses subtle psychological tricks to influence users' behavior by using contrasting visual prominence to steer users into making a certain selection, such as bright colors or bold fonts to make certain options stand out more than others.
· ***Overloading***: A business sends users numerous requests or offers numerous options in order to deter certain actions or manipulate users to unintentionally share or allow the processing of their personal data.
· ***Skipping***: A user interface is designed to cause users to forget or overlook data protection concerns or options.
· ***Shaming*** or ***Stirring***: A business manipulates user choice with emotional steering, e.g. an option to decline is worded in such a way as to shame the user into compliance.
· ***Hindering***: The user experience includes dead end choices or other tactics that make it difficult or impossible for users to obtain information or take action.
· ***Fickle***: These practices include disguised ads and inconsistent user interfaces that are confusing or unclear.
· ***Left in the Dark***: Interfaces are designed to hide choice from users or include ambiguous wording, such as conflicting information about how personal information is being processed.[4]

02
EXAMPLES OF DARK PATTERNS

Dark patterns are often used in:

· ***Negative Options***: An online provider employing dark patterns may make the process for purchasing a subscription online relatively easy with a short check-out/purchase flow, but establish a complex, multistep flow process, online or offline, for cancel-

2 See *In the Matter of Epic Games, Inc.* (March 14, 2023), available at https://www.ftc.gov/legal-library/browse/cases-proceedings/1923203-epic-games-matter.

3 See https://www.deceptive.design/about-us (last accessed April 30, 2023).

4 European Data Protection Board ("EDPB"), *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognize and avoid them* (March 14, 2022), available at https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf; Federal Trade Commission, *Bringing Dark Patterns to Light* (September 2022), available at https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

ling the subscription which involves forcing customers to consider different offers designed to prevent them from un-subscribing.

· ***Online Advertising***: A business uses deceptive tactics to cause users to click on ads, such as a fake news article or headline.

· ***Dark Patterns in E-commerce***: An e-tailer uses deceptive tactics designed to cause users to buy more products than intended. For example, a business might use a "buy now, pay later" option or presenting a limited time offer that has no actual deadline or that resets at an arbitrary time (e.g. the limited time offer clock resets when the user refreshes the webpage).

· ***Consumer Ratings***: A "neutral" shopping comparison site ranks choices based on compensation not actual experiences with a product or using phony customer endorsements or presenting other people's experience without revealing material information, such as compensating endorsers or not qualifying an endorser's experiences as atypical.

> ***"Dark patterns are highly effective at influencing consumer behavior, particularly with less sophisticated users and when layered together***

Dark patterns not only harm individual consumes; they also are anticompetitive. Businesses using dark patterns gain an unfair advantage over competitors by, for example, making fair and accurate price and service comparison difficult because information is hidden or deceptively presented. Businesses may also use dark patterns to prevent consumers from switching to competitors (which may offer better prices or services) by making cancellation difficult, e.g. presenting a "Keep Your Benefits" option as a bright orange button, while presenting the "Cancel Subscription" option as a smaller font, pale gray hyperlink.

03
REGULATORY DEVELOPMENTS IN THE U.S.

Regulators in the U.S. have long targeted unfair and deceptive practices designed to manipulate consumers in certain ways. The digital world is no different.

A. Dark Patterns and Consumer Protection

In September 2020, the Federal Commission announced a $10 million settlement against an online subscription service that operated a deceptive subscription program that inadequately disclosed that 12-month memberships and extensions on 30-day free trial memberships at reduced rates would automatically renew and, despite advertising "easy cancellation," made cancellations nearly impossible. While the settlement did refer to these practices as dark patterns, then FTC Commissioner (and current Director of the Consumer Financial Protection Bureau ("CFPB")) Rohit Chopra issued a statement calling the business practices dark patterns.[5] In the statement, Commissioner Chopra noted: "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." Director Chopra continues to investigate allegations of digital dark patterns while at the helm of the CFPB.[6] Since then, the Federal Trade Commission ("FTC") released a September 2022 Staff Report, *Bringing Dark Patterns to Light* ("FTC Report").[7] The FTC has finalized enforcement actions against businesses using dark patterns.[8]

5 Federal Trade Commission, Statement of Commissioner Rohit Chopra, *Regarding Dark Patterns in the Matter of Age of Learning, Inc. Commission File Number 1723186* (September 2, 2020), available at https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf.

6 See "CFPB Issues Guidance to Root Out Tactics Which Charge People Fees for Subscriptions They Don't Want" (January 19, 2023), available at https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-guidance-to-root-out-tactics-which-charge-people-fees-for-subscriptions-they-dont-want/ (last accessed April 30, 2023).

7 Federal Trade Commission, *Bringing Dark Patterns to Light* (September 2022), available at https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

8 See e.g. Credit Karma, LLC, available at https://www.ftc.gov/legal-library/browse/cases-proceedings/2023138-credit-karma-llc; RagingBull.com, available at https://www.ftc.gov/legal-library/browse/cases-proceedings/2023073-ragingbullcom; and LendingClub Corporation, available at https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3088-lendingclub-corporation.

Consumer protection laws are not the only options for federal and state regulators seeking to prevent dark patterns. For example, the Restore Online Shopper's Confidence Act ("ROSCA"), a 2012 law targeted to online negative option plans, requires (*inter alia*) clear and conspicuous disclosures of material terms prior to requesting and receiving a customer's billing information for a recurring charge.[9] Effective as of July 1, 2022, California's now-updated automatic renewal law requires that a business provide its California consumers an online subscription cancellation option for a subscription purchased online, without extra steps that obstruct terminating the autorenewal plan.[10] Colorado, Illinois, Maryland, and New York also updated their automatic renewal/negative option laws recently to impose more robust notice and cancelation requirements on businesses offering autorenewal plans.

> ***Consumer protection laws are not the only options for federal and state regulators seeking to prevent dark patterns***

In April 2023, the FTC proposed substantial amendments to the existing Negative Option Rule, setting higher standards for autorenewal promotions and sales than exist under current federal or state laws and regulations.[11] If promulgated, the revised Negative Option Rule will apply to many more businesses and scenarios than are currently subject to autorenewal regulation. The proposed Negative Option Rule would cover all forms of so-called "negative option" marketing and sales in all media, including negative options sold in a business-to-business ("B2B") context (e.g. autorenewal terms in business services contracts), for month-to-month auto-renewing terms (e.g. "no contract" cell, Internet, media or entertainment services and even auto-renewing monthly residential and commercial real estate tenancies) and for both the sale of goods and services. Other notable additions to the Negative Option Rule include enhanced disclosure, consent, and cancellation requirements, as well as a powerful misrepresentation prohibition and annual reminders. Whether or not this proposed Negative Option Rule is finalized by the FTC, it clearly shows that regulators are targeting dark patterns in every sphere of the marketplace.

B. Dark Patterns and Privacy

State privacy laws are also targeting dark patterns. The amended California Consumer Privacy Act ("CCPA"), which will be fully enforced July 1, 2023, targets dark patterns used in the process offered to consumers for opting out of the sale and sharing of personal information, among other areas.[12] For example, the consent web page must "allow[] the consumer . . . to revoke the consent as easily as it is affirmatively provided."[13] The link to the consent web page cannot "not degrade the consumer's experience on the web page the consumer intends to visit and has a similar look, feel, and size relative to other links on the same web page."[14] The regulations implementing the CCPA, as amended by the California Privacy Rights Act ("CPRA"), go even further and state, "[a] business's intent in designing the interface is not determinative in whether the user interface is a dark pattern, but a factor to be considered."[15]

These requirements are directly targeting dark patterns used by businesses to influence consumer behavior and prevent a consumer from making a fully informed decision about consenting to the business's sale or sharing of the consumer's personal information. Of importance, consent obtained through dark patterns does not constitute "consent" under the CCPA. Dark patterns also are addressed in the Colorado Privacy Act ("CPA"), which specifically defines "consent" as not including an "agreement obtained through dark patterns"[16] and the Connect-

9 Restore Online Shopper's Confidence Act, 15 U.S.C. §§ 8401—8405.

10 California Business and Professions Code §§ 17600—17606.

11 Federal Trade Commission, *Negative Option Rule, A Proposed Rule by the Federal Trade Commission* (April 24, 2023), 88 Federal Register 24716.

12 California Civil Code §§ 1798.100—1798.199.100.

13 Cal. Civ. Code § 1798.135(b)(2)(A).

14 Cal. Civ. Code § 1798.135(b)(2)(B).

15 California Code of Regulations Title 11 § 7004(c).

16 Colorado Revised Statutes §§ 6-1-1301—6-1-1313 (effective July 1, 2023).

icut Data Privacy Act which defines dark pattens similarly to CCPA and CPA but also includes "any practice the Federal Trade Commission refers to as a 'dark pattern.'"[17] Like California, under the Colorado[18] and Connecticut[19] laws, consent obtained through the use of dark patterns is not valid.

While not specifically targeted to dark patterns, the California Age-Appropriate Design Code Act ("CAADCA") addresses dark patterns affecting interactions with minors.[20] Under the CAADCA, businesses are prohibited from "us[ing] dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature to forego privacy protections, or to take any action that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or well-being."[21] Other states are considering laws similar to CAADCA.[22]

And of course, the mini-FTC Acts enforced by the states establish broad powers for the relevant agencies to regulate unfair or deceptive acts and practices – including dark patterns.

In Europe, dark patterns also may violate various provisions of the General Data Protection Directive ("GDPR"),[23] including the fairness and transparency principle (Art. 5(1)(a)), the accountability principle (Art. 5(2)), data protection by design and default (Art. 25), the requirement to provide transparent privacy notices to data subjects (Art. 12(1), 13 & 14), and the data subject rights under GDPR Art. 15-22. Further, Europe's Digital Services Act, which applies to online-platforms, also decrees that "[r]ecipients of a service should be able to make a free, autonomous and informed decisions or choices when using a service and providers of intermediary services shall not use any means, including via its interface, to distort or impair that decision-making. In particular, recipients of the service should be empowered to make decisions, inter alia regarding the acceptance of and changes to terms and conditions, advertising practices, privacy and other settings, recommender systems when interacting with intermediary services."[24] Thus, no matter the medium, regulators are concerned with dark patterns in consumer interactions and are working to prohibit their use.

> ***"While not specifically targeted to dark patterns, the California Age-Appropriate Design Code Act ("CAADCA") addresses dark patterns affecting interactions with minors***

Dark patterns are also an issue addressed by self-regulatory agencies in the United States. The Network Advertising Industry ("NAI"), which has previously covered regulatory action on dark patterns,[25] published guidance for its members on the topic and issued opinions.[26] Of note, the NAI addresses "light patterns" which "are practices that make proactive decisions on behalf of users, having their best intentions in mind." These practices should also be reviewed carefully, with the goal that the light pattern only advances the user's ability to make informed choices, and does not make the choice on their behalf. A light pattern may evolve into a dark pattern if the business begins to "make assumptions about what is in consumers' best in-

17 State of Connecticut, Public Act No. 22-15, § 1(11).

18 Colorado Revised Statutes § 6-1-1303(5).

19 State of Connecticut, Public Act No. 22-15, § 1(6).

20 Cal. Civ. Code §§ 1798.99.28-1798.99.40.

21 Cal. Civ. Code § 1798.99.31(b)(7).

22 See e.g. Maryland Age-Appropriate Design Code Act, HB0901, § 14-4507(7).

23 Regulation 2016/679.

24 Digital Services Act, 2020/0361(COD), Recital 39a.

25 See https://thenai.org/dark-and-light-patterns-when-is-a-nudge-a-problem/.

26 Network Advertising Industry comments filed with the Federal Trade Commission, *Bringing Dark Patterns to Light: An FTC Workshop* (March 15, 2021), available at https://thenai.org/wp-content/uploads/2021/07/nai_comments_ftc_dark_patterns_15march2021.pdf; see also National Advertising Division Recommends Pier 1 Imports Clearly and Conspicuously Disclose Material Terms of Pier 1 Rewards Membership (February 27, 2023), available at https://bbbprograms.org/media-center/dd/pier-1-rewards (last accessed April 30, 2023).

terests run the risk of promoting certain business models over others."[27]

04

HOW TO PROTECT YOURSELF FROM DARK PATTERNS

To reduce the risk of regulatory sanctions, the potential for consumer class actions and reputational damage, online platforms and publishers should be mindful of the increasing focus on dark patterns by U.S. and European regulatory authorities. Best practices include:

· Evaluate current practices to ensure that marketing and website interface design teams are aware of the regulatory risks and requirements.
· Make use of interdisciplinary teams when designing a user experience, including designers, privacy professionals, and decision-makers.
· Consider the audience in designing the user interface. Design for adults, teens, and children may differ.
· Design consent processes to ensure that consent is informed, specific, affirmative, and voluntary.
· Ensure that material terms and conditions are clear, conspicuous, and relevant. The language should be direct, clear and not used to pressure or manipulate consumers into making preferred (by the business) choices.
· Provide accurate and complete information from the start and maintain the information as accurate and complete through the consumer's experience so that consumers are not misinformed or misled.
· Use fair and transparent disclosures presented at or before the consumer action is required, and highlight unusual or unexpected practices.
· View the disclosures from the audience's perspective.
· Check that privacy policies and website terms accurately describe current data practices in a manner that is understandable to the typical consumer.
· Implement Privacy by Design principles and proactively integrate privacy into the design and architecture of systems and business practices. In particular, practice data minimization and collect only the information that you need and focus on transparency.
· Opt-in and opt-out flows should clearly disclose what consumers are opting in and out of, require a similar number of steps (i.e. not make it harder to opt out than to sign up), and be easily accessible to consumers.
· Review consumer concerns regarding the user flow and remedy any identified potential issues as soon as possible.

> ***Provide accurate and complete information from the start and maintain the information as accurate and complete through the consumer's experience so that consumers are not misinformed or misled***

As a consumer, you can protect yourself from dark patterns:

· Be aware of the different types of dark patterns that exist. The more you know about dark patterns, the easier it will be to spot them.
· Take your time when reading any terms of service or other agreements. Don't just click "agree" without reading the fine print.
· Don't be afraid to ask questions if you don't understand something. If you're not sure what a business is asking you to agree to, ask them to explain it in plain English.
· Report dark patterns to the business involved. If you see a dark pattern, you can report it to the business involved. You can also file a complaint with your local consumer protection agency.

27 Digital Services Act, Regulation (EU) 2022/2065, Recital 39a.

05
CONCLUSION

Dark patterns are a form of deceptive design that can harm consumers. Awareness of the different types of dark patterns and taking steps to protect your business and consumers can help to reduce risk by focusing on offering consumers the information and experience needed to make fully informed decisions.

Dark patterns are a form of deceptive design that can harm consumers

TACKLING DARK PATTERNS: HOW TO REASONABLY PREVENT CONSUMER MANIPULATION AND COMPETITION DISTORTIONS?

BY FRÉDÉRIC MARTY

& JEANNE TORREGROSSA

Respectively CNRS – GREDEG – Université Côte d'Azur ; OFCE – Sciences Po., Paris ; CIRANO, Montréal and Altermind.

Dark patterns, widely acknowledged to amount to manipulative practices, have been fiercely debated during the Digital Services Act negotiations. They have been added to the already long list of issues facing the digital economy. But what exactly is behind them?

The OECD provides a definition which captures the relatively broad scope of all the practices that could be covered by this term. It defines them as "user interfaces used by some online businesses to lead consumers into making decisions they would not have

otherwise made if fully informed and capable of selecting alternatives."[2]

Sketching out a more precise definition of dark patterns first requires separating them from their nearest equivalents in the "old world," namely marketing. A deceptive interface aims to "manipulate the consumer into doing something that is inconsistent with their preferences, in contrast to marketing efforts that are designed to alter those preferences."[3] These so-called "deceptive and manipulative" interfaces have been proliferating for years and every internet user has encountered them online.

The best-known examples are "hidden subscriptions" ("the consumer incurs a recurring fee under the pretense of a one-time fee or a free trial period"),[4] "hidden costs ("new, additional, and often unusually high charges are added just before a consumer is about to complete a purchase"),[5] or "pressured selling" ("defaults or high-pressure tactics that steer consumers into purchasing a more expensive version of a product (upselling) or related products (cross-selling)").[6]

The academic literature has addressed this broad and multidisciplinary subject for many years now. While the initial aim was to achieve a good technical understanding of the phenomenon,[7] the aim today is to grasp its underlying mechanisms and actual impact on consumers and competition. It is therefore necessary to determine the extent of the problem and – above all – to assess, as with many new phenomena, the necessity of laying down specific regulations while guaranteeing their expected effectiveness and potential side-effects.

Mechanically, these misleading interfaces have not escaped the vigilance of the competition and regulatory authorities. The UK competition authority, the Competition and Markets Authority ("CMA"), at the vanguard on many online issues, opened an investigation in November 2022 into the online practices of the company Emma Sleep concerning so-called "pressured selling"[8] techniques. It identified the existence of time-limited urgent offers or countdowns in advertisements that would, for example, lead consumers to believe that the discount obtained would no longer be valid at the end of the indicated period, thus forcing them to make their purchase quickly without a fully informed choice.[9] This investigation is part of the CMA's wider work to focus some of its forces on manipulative online sales practices, "Online Architecture Choice"[10] and a program to help consumers spot these sales techniques, "Rip off Tip off."[11]

Sketching out a more precise definition of dark patterns first requires separating them from their nearest equivalents in the "old world," namely marketing

These two major UK initiatives, aimed at curbing practices while raising consumer awareness about them, echo the recent survey conducted by the European Commission and national consumer protection authorities on online sales techniques with rather alarming results: out of 399 online shops surveyed, 148 contained at least one sales technique that can be considered as a dark pattern - fake countdowns, manipulative consumer guidance or hidden information.[12]

2 OCDE, Roundtable on Dark Commercial Patterns Online, Summary of discussion, (February 19, 2021).

3 Jamie Luguri & Lior J. Strahilevitz, *Shining a Light on Dark Patterns*, Journal of Legal Analysis, 13(1), pp.43–109, (2021).

4 OCDE, Roundtable on Dark Commercial Patterns Online, Summary of discussion, (February 19, 2021).

5 OCDE, Roundtable on Dark Commercial Patterns Online, Summary of discussion, (February 19, 2021).

6 OCDE, Roundtable on Dark Commercial Patterns Online, Summary of discussion, (February 19, 2021).

7 Michael Toth, Nataliia Bielova & Vincent Roca, *On dark patterns and manipulation of website publishers by CMPs*, Proceedings on Privacy Enhancing Technologies (PoPETs), pp.478–497, (2022).

8 OCDE, Roundtable on Dark Commercial Patterns Online, Summary of discussion, (February 19, 2021).

9 Press Release, Competition and Markets Authority, CMA investigates online selling practices based on 'urgency' claims (November 30, 2022).

10 Competition and Markets Authority, Online choice architecture work (November 30, 2022).

11 Press Release, Competition and Markets Authority, 7 out of 10 people have experienced potential rip-offs online, worrying new CMA research reveals (February 9, 2022).

12 Press Release, European Commission, Consumer protection: manipulative online practices found on 148 out of 399 online shops screened (January 30, 2023).

The setting up and development of these interfaces, which are now under the scrutiny of the authorities, have, as Yeung (2017) mentions, their origin in two well-known phenomena: massive data and algorithms.[13] The author stresses that this data is collected only to become a valuable and exploitable asset, thus pointing to one of the most significant issues of the digital economy. To become valuable and exploitable, Yeung (2017) points out that these data must be inserted into a much broader combination of predictive process and information processing technology to arrive at what can be called "machine learning" creating logical links far beyond what the human mind can do.

> ***These two major UK initiatives, aimed at curbing practices while raising consumer awareness about them***

It is no longer a question of moving into an information economy as it was previously understood, but into a prediction economy based on efficient data collection and processing. Deceptive or non-deceptive interfaces are for traditional sales techniques what targeted advertising was and still is for contextual advertising: a major disruption based on the ability to collect and exploit data.

Whether it is advertising or interfaces, the place of information in the economy is continually being redesigned, under the effect of the digitalization of the economy, to reveal some of its hitherto hidden dimensions. Whereas contextual advertising - historically used for instance in print or broadcast media - was limited to choosing the advertisement to be shown according to the context in which the advertising content was inserted, targeted advertising identifies people individually to deliver specific advertising messages to them based on their idiosyncratic characteristics. While the former technique does not require any information about the consumer, the effectiveness of the latter depends almost entirely on the level of information held about the user and its processing.

The sharing and possession of information are decisive here. They have always been the keystone of markets: the consumer must know to choose, and the company must know its consumers to offer products that meet their needs. However, they are also the subject of a very difficult balance to strike: too much information exchanged between companies - or made available - can lead to explicit or tacit collusion between them, and too much information about the consumer can jeopardize his welfare. The digital economy and the development of artificial intelligence exacerbate these issues.

In this way, considering the issues related to dark patterns is a matter of both consumer and competition protection. At consumer level, they raise issues in terms of reducing the scope of available choices and personalized and dynamic manipulation of preferences. They can give rise to practices which are even more damaging as the consumers exposed are vulnerable.[14] The lower the level of consumer expertise and information, the easier it will be to implement manipulative strategies. Not only can dark patterns enable online players to extract an additional share of consumer surplus, but they can also reduce the consumer's ability to exercise sovereignty by hindering the comparison of offers between rival firms or to measure the costs and constraints associated with a switching decision. Dark patterns can therefore develop even more easily when consumers have already opted for single-homing strategies and when the digital ecosystem at stake presents strong immersive characteristics.

From a competition law and economics perspective, dark patterns can lead to inter-ecosystems and intra-ecosystem competition concerns.

In the context of inter-ecosystems competition, they may lessen the competitive pressure exerted by competitors and, to a certain extent, introduce the vector of unfair competition as they involve biased information on the characteristics of the products offered or manipulative techniques. In other words, to quote Rohit Chopra's dissenting opinion in the *Zoom* case dealt with the FTC: "deception distorts competition."[15] In this case, the company was accused of not respecting its commitments in terms of encrypting calls. To generalize this, we could say that the companies that make the most use of dark patterns could have a competitive advantage over their competitors. The incentives would then move towards a downward alignment: the large ecosystems would all have an interest in unilaterally mak-

13 Karen Yeung, *'Hypernudge': Big Data as a mode of regulation by design*, Information, Communication & Society, 20(1), pp.1–19 (2017).

14 Renu Isidore R. & Christie P., *The relationship between the income and behavioural biases*, Journal of Economics, Finance and Administrative Science, 24 (47), pp.127–144 (2019).

15 Federal Trade Commission, Dissenting Statement of Commissioner Rohit Chopra Regarding Zoom Video Communications, Inc., (November 6, 2020).

ing their offerings less transparent and more confusing for consumers.[16]

As for intra-ecosystem competition, dark patterns can reinforce the effectiveness of self-preferencing strategies by drawing consumers towards a particular offer. They could therefore effectively make it possible either to exclude an as-efficient and possibly more attractive competitor, by artificially reducing its visibility or by diverting consumers from its offer,[17] or to implement exploitative strategies by forcing some of its commercial partners to contract for additional services to escape a possible demotion, which is particularly difficult to evidence in litigation.[18]

As for intra-ecosystem competition, dark patterns can reinforce the effectiveness of self-preferencing strategies by drawing consumers towards a particular offer

Two examples of such architectures and their impacts can be mentioned. Firstly, drip-pricing practices are well known, and their effects have long been evaluated in the academic literature, as shown by the work of Blake et al. published in 2021.[19] The latter showed through an experiment that abandoning such strategies can lead to a 28 percent loss of revenue for an online vendor. Secondly, in the domain of retail banking fees, a White House press release of February 1, 2023 on the proposed Junk Fee Prevention Act illustrates the burden of these "Unfair and Costly Junk Fees" on the most vulnerable consumers who are most exposed to manipulative practices.[20] In the field of banking services, two reports published in 2021 by the CFPB (Consumer Financial Protection Bureau) show that not only do these unanticipated fees have a significant impact on consumer welfare, they also reduce competition between banking institutions by impeding the transparency necessary for price competition.[21]

All of these factors demonstrate that there is a legitimate concern surrounding dark patterns, but this should not obscure a certain number of risks and limits that need to be taken into consideration in terms of public policy design.

Firstly, personalization is not a competitive problem as such. Personalized recommendations, especially based on algorithmic predictions grounded on massive data collection and processing, contribute to economic efficiency and consumer satisfaction. Directing consumers towards a particular choice can reduce transaction costs and collectively lead to efficiency gains through volume or scale effects. Secondly, nudges and sludges can have desirable effects not only collectively but also individually. They can help to counteract existing biases in favor of the usual suppliers. They can thus help to defend consumers against themselves, for example when they exhibit addictive behavior or excessive aversion to change, which may lead them not to seek out competition when they should. It can help to overcome consumer inertia.[22]

Secondly, dark patterns are not the exclusive privilege of dominant digital firms. They may be implemented in brick-and-mortar stores (albeit with less efficiency and refinement). They can also be implemented by non-dominant operators. Indeed, dark patterns can be developed by operators who do not have a data advantage or specific artificial intelligence capabilities. Dark patterns expose consumers to the risk of being harmed by non-dominant market players.

While it is therefore legitimate to be concerned about dark patterns, possible remedies should be carefully considered.

Firstly, dark patterns are not exclusive to "gatekeepers" in the sense of the Digital Markets Act. They can hardly be remedied by asymmetric regulation. However, any symmet-

16 Robert Edwards, *Pricing and obfuscation with complexity adverse consumers*, Oxford Economic Papers, 71(3), pp.777–798, (2019).

17 Patrice Bougette, Axel Gautier & Frédéric Marty, *Business Models and Incentives: For an Effects-Based Approach of Self-Preferencing?*, Journal of Competition Law and Practice, 13(2), pp.136–143, (2022).

18 Frédéric Marty, *From Demoting to Squashing? Competitive Issues Related to Algorithmic Corrections: An Application to the Search Advertising Sector*, Competition Policy International (April 2019), https://www.competitionpolicyinternational.com/wp-content/uploads/2019/04/CPI-Marty.pdf

19 Tom Blake, Sarah Moshary, Kane Sweeney & Steve Tadelis, *Price Salience and Product Choice*, Marketing Science, 40(4), pp. 619–636 (2021).

20 The White House, Fact Sheet : President Biden highlights new progress on his competition agenda, (February 1, 2023).

21 Consumer Financial Protection Bureau, Office of Research Publication, Data Point: Overdraft/NSF Fee Reliance Since 2015 – Evidence from Bank Call Reports, (December 1, 2021).

22 Competition and Markets Authority, Tackling the loyalty Penalty, (September 28, 2018).

rical regulation can have a negative effect on competition insofar as the costs of compliance weigh relatively more on small players than on large ones. This is the case for the GDPR and will be even more so with the interoperability requirements contained in the draft Data Act. Overly intrusive regulation that is imposed on all players may have the effect of strengthening the competitive position of the most powerful.

Secondly, even from the sole perspective of consumer protection, the prevention and sanctioning of dark patterns require substantial means of investigation. While blatantly manipulative procedures must be prohibited *per se*, a balancing approach is necessary for certain patterns in that the personalization of the offer can only be envisaged through an effects-based approach.

Thirdly, a socially responsible company, regarding all its stakeholders and more precisely its most vulnerable consumers, could refrain from implementing commercial practices based on the delivery of biased information or manipulative choice architecture. The absence of dark patterns could therefore be integrated into an ethical approach and a compliance policy. These can respond to the intrinsic motivations of the firm but also to extrinsic motivations linked to the possible reputational cost that could result from the exposure of such practices and their effects. Within this framework, the recommendations formulated as regards algorithmic liability could be extended to dark patterns:[23] A firm that implements an algorithm has a clear interest in investing in risk prevention both *ex ante* and as it is used. Procedures involving the certification of choice architectures and periodic audits could be part of self-regulation measures that complement public supervision policies that expose firms when they are not very careful about how the effects of their practices could lead to sanctions.

> ***While it is therefore legitimate to be concerned about dark patterns, possible remedies should be carefully considered***

23 Nathalie De Marcellis-Warin, Frédéric Marty, Eva Thelisson & Thierry Warin, *Artificial intelligence and consumer manipulations: from consumer's counter algorithms to firm's self-regulation tools*, AI & Ethics, 2(2), pp.259–268, (2022).

WHAT'S **NEXT**

For June 2023, we will feature a TechREG Chronicle focused on issues related to ESG.

ANNOUNCEMENTS

CPI TechREG CHRONICLES July 2023

For July 2023, we will feature a TechREG Chronicle focused on issues related to **Telemedicine**.

Contributions to the TechREG Chronicle are about 2,500 – 4,000 words long. They should be lightly cited and not be written as long law-review articles with many in-depth footnotes. As with all CPI publications, articles for the CPI TechREG Chronicle should be written clearly and with the reader always in mind.

Interested authors should send their contributions to Sam Sadden (ssadden@competitionpolicyinternational.com) with the subject line "TechREG Chronicle," a short bio and picture(s) of the author(s).

The CPI Editorial Team will evaluate all submissions and will publish the best papers. Authors can submit papers in any topic related to competition and regulation, however, priority will be given to articles addressing the abovementioned topics. Co-authors are always welcome.

ABOUT US

Since 2006, **Competition Policy International** ("CPI") has provided comprehensive resources and continuing education for the global antitrust and competition policy community. Created and managed by leaders in the competition policy community, CPI and CPI TV deliver timely commentary and analysis on antitrust and global competition policy matters through a variety of events, media, and applications.

As of October 2021, CPI forms part of **What's Next Media & Analytics Company** and has teamed up with **PYMNTS**, a global leader for data, news, and insights on innovation in payments and the platforms powering the connected economy.

This partnership will reinforce both CPI's and PYMNTS' coverage of technology regulation, as jurisdictions worldwide tackle the regulation of digital businesses across the connected economy, including questions pertaining to BigTech, FinTech, crypto, healthcare, social media, AI, privacy, and more.

Our partnership is timely. The antitrust world is evolving, and new, specific rules are being developed to regulate the so-called "digital economy." A new wave of regulation will increasingly displace traditional antitrust laws insofar as they apply to certain classes of businesses, including payments, online commerce, and the management of social media and search.

This insight is reflected in the launch of the **TechREG** Chronicle, which brings all these aspects together — combining the strengths and expertise of both CPI and PYMNTS.

Continue reading CPI as we expand the scope of analysis and discussions beyond antitrust-related issues to include Tech Reg news and information, and we are excited for you, our readers, to join us on this journey.

Scan to Stay Connected!

Scan here to subscribe to CPI's **FREE** daily newsletter.

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