Received: 10 November 2023 | Accepted: 13 November 2023

DOI: 10.1111/eulj.12478

VARIETY: ORIGINAL ARTICLE

WILEY

The collective welfare dimension of dark patterns regulation

Fabiana Di Porto* | Alexander Egberts**

Abstract

Dark Patterns are interface design elements that can influence users' behaviour in digital environments. They can cause harm, not only on an individual but also a collective level, by creating behavioral market failures, reducing trust in markets and promoting unfair competition and data dominance. We contend that these collective effects of Dark Patterns cannot be tackled by existent laws, and thus call for policy intervention. This article reviews how existing and proposed laws in Europe and the US, namely the EU Digital Services Act and Digital Markets Act as well as the U.S. DETOUR and AICO Acts, address these collective dimensions of welfare and add to existing protection. We find that the novel legislative measures attain that goal to varying degrees. However, the collective welfare perspective may prove useful to both support a risk-based approach to the enforcement and provide guidance as to which practices should be addressed as priority.

1 | INTRODUCTION

Dark Patterns are elements of user interface design,[1] which steer the user towards engaging in or refraining from a certain action, the result of which usually aligns with the interest of the architect of the digital surrounding.[2] Examples include adding unwanted products into the customer's digital shopping basket without informing them,[3]

* Fabiana Di Porto is Professor of Law and Technology, University of Salento and LUISS University, Rome. Member of the Executive board of the Academic Society for Competition Law (ASCOLA). Former Forcheimer Visiting Professor, Law Faculty, Hebrew University of Jerusalem (2019/20).

** Alexander Egberts is a Research Fellow at the Max Planck Institute for Research on Collective Goods, Bonn.

Both authors jointly conceived this article and drafted the Introduction and Conclusion. Fabiana Di Porto wrote Ch. 3, 5 and 6.2; Alexander Egberts wrote Ch. 2, 4, and 6.1.

The authors did not receive any sources of funding or in-kind support in the preparation of this article; they have no conflict of interests to disclose.

[1] User interface design focuses on how information is presented in digital human–computer interfaces and is part of user experience design: D. Norman and J. Nielson, The Definition of User Experience (UX) (2023), retrievable at https://www.nngroup.com/articles/definition-user-experience.

[2] Although they both use choice architecture to influence behaviour, Dark Patterns differ from "nudges"; see R. Thaler and C. Sunstein, *Nudge: Improving Decisions About Health, Wealth and Happiness* (HarperCollins, 2008): with nudges individuals are helped to take decisions that are more in line with their (assumed) self-interest; with Dark Patterns, on the contrary, users are made to behave in a particular way for the benefit of the choice architect.

[3] A practice known as the "Sneak intoBasket" pattern: J. Luguri and L. Strahilevitz, 'Shining a Light on Dark Patterns', (2021) 13 *Journal of Legal Analysis*, 43, 67.

preventing users from cancelling ongoing subscriptions,[4] or tricking them into giving consent to the processing of their data.[5] These design elements can be found in all kinds of digital systems, such as websites, mobile applications, computer software or even operating systems. Usually, through Dark Patterns the user is manipulated to either disclose more of their personal data, buy greater amounts of goods or services, or spend more time within a specific system.[6] The term 'Dark Patterns'—after being introduced in a blogpost by British UX designer Harry Brignull[7]—quickly took on and received a lot of attention from media outlets, interest groups and social media channels. Although it has also met criticism,[8] the phrase has become established in several academic circles[9] and has finally been adopted by legislators.[10]

The normative accusation against such design practices is that they systematically abuse users' cognitive biases and heuristics to induce them to behave in a way that is contrary to their actual preferences.[11] In other words, the "darkness" of the design lies in the fact that operators employ them to influence the user to act against their own interests, and therefore erode their ability to make rational and autonomous decisions. This has triggered the concern of policymakers and regulatory authorities in the EU,[12] as well as in the US,[13] who have explicitly acknowledged a need for action.

As a result, both the EU and the US are currently working on legislative measures designed to reduce the use of deceptive designs. In the US through the American Innovation and Choice Online (AICO) Act and the Deceptive Experiences to Online Users Regulation (DETOUR) Act.[14] In the EU, Dark Patterns are addressed in the Digital Markets Act (DMA) and the Digital Services Act (DSA), which are already force.[15] In fact, the phenomenon is not

[4]An example of "Roach Motel" pattern: Luguri and Strahilevitz, above, n. 3.

[5]See A.E. Waldman, 'Cognitive Biases, Dark Patterns, and the "Privacy Paradox"', (2020) 31 *Current Opinion in Psychology*, 105, who focuses on cognitive biases and the significance of the privacy paradox; see also C.M. Gray et al. 'Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective' (2021), *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (providing an interdisciplinary assessment of Dark Pattern legality in cookie banners).

[6]See, e.g., A. Mathur, J. Mayer and M. Kshirsagar, 'What Makes a Dark Pattern … Dark? Design Attributes, Normative Considerations, and Measurement Methods', (2021) *CHI Conference on Human Factors in Computing Systems*, 1–18, retrievable at https://doi.org/10.1145/3411764.3445610. This and all following online materials were last retrieved on 10 November 2023.

[7]Originally, Brignull defined Dark Patterns as 'bad design patterns [which have] been crafted with […] a solid understanding of human psychology, to trick users into doing things they wouldn't otherwise have done', see H. Brignull, 'Dark Patterns: Dirty Tricks Designers Use to Make People Do Stuff', (2010) *Blogpost*, retrievable at https://90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/.

[8]The term has been criticised for reproducing colonialist thought structures, see C. Sinders. 'What's in a Name? Unpacking Dark Patterns versus Deceptive Designs', (2022) *Blogpost*, retrievable at https://medium.com/@carolinesinders/whats-in-a-name-unpacking-dark-patterns-versus-deceptive-design-e96068627ec4.

[9]In computer science, see, e.g., C. Gray, Y. Kou and B. Battles. 'The Dark (Patterns) Side of UX Design', (2018) *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, Paper No. 534; in psychology, see, e.g., Waldman, above, n. 5; in law, see, e.g., M.R. Leiser and M. Caruana, 'Dark Patterns: Light to be Found in Europe's Consumer Protection Regime', (2021) *Journal of European Consumer and Market Law*, 237; in philosophy, see, e.g., S. Ahuja and J. Kumar, 'Conceptualizations of User Autonomy within the Normative Evaluation of Dark Patterns', (2022) 24 *Ethics and Information Technology*, 52, to name just a few.

[10]See, e.g., Recital 67 DSA, below, Section 4.1.1.

[11]See Mathur et al., above, n. 6; Waldman, above, n. 5; R. Calo, 'Digital Market Manipulation', (2014) 82 *George Washington Law Review*, 995; Luguri and Strahilevitz, above, n. 3.

[12]F. Lupiáñez-Villanueva et al., 'Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation: Final Report', (2022) *EU Commission Policy Paper*, retrievable at https://data.europa.eu/doi/10.2838/859030 (hereinafter: EU Dark Patterns Report 2022), 30, 32, 58, 64; European Commission, 'Guidance on the Interpretation and Application of Directive 2005/29/EC', (2021) *EU Commission Policy Paper*, 4.2.7; European Data Protection Board, 'Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces', (2022), *EU Policy Paper*, retrievable at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en (hereinafter: EDPB Guidelines 2022).

[13]See US Federal Trade Commission, '"Bringing Dark Patterns to Light" Workshop', (2021), *Workshop Proceedings*, retrievable at https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop. For the EU, see the Commission Notice concerning unfair business-to-consumer commercial practices in the internal Market, 2021/C526/01, 99–102.

[14]The US has proposed two bills in the 116th and 117th congressional session which address Dark Patterns: The American Innovation and Choice Online Act ("AICO") H.R. 3816 American Innovation and Choice Online Act (hereinafter "AICO Act") 2021, 117th Congress (2021–2022) (available at https://www.congress.gov/bill/117th-congress/house-bill/3816/text) paired with S.2992, 117th Congress (2021–2022) (available at https://www.congress.gov/bill/117th-congress/senate-bill/2992); and the Deceptive Experiences to Online Users Reduction ("DETOUR") Act, H.R. 6083, 117th Congress (2021–2022), S. 3330, on 7 December 2021. The DETOUR Act has been reintroduced to the 118th congressional session on 27 July 2023, retrievable at https://www.congress.gov/bill/118t-hcongress/senat-ebill/2708.

[15]Digital Markets Act (DMA): Regulation (EU) no. 2022/1925, 12 October 2022 (the DMA has become applicable from 2 May 2023). Digital Services Act (DSA): Regulation (EU) no. 2022/2065 (entered into force on 16 November 2022, and to become applicable as of 1 January 2024).

completely novel: on both sides of the Atlantic, Dark Patterns have hitherto been regulated by consumer and data protection laws, which aim to ensure equitable online interactions between businesses and users.[16]

Those existing regulations on Dark Patterns have been united in their conceptual approach of *protecting individual welfare*,[17] meaning that they aim at safeguarding the decision-making process of individuals—both in their role as (intermediate and final) consumers and data subjects—from external influence.[18] By so doing, these regulations aim at allowing users to act more rationally and in accordance with their relative preferences, so to maximise the benefits they can reap from online transactions, without being subject to unfair conduct and undue influences from their business counterparts.[19] While preserving the ability of individuals to act in accordance with their preferences and maximise their welfare freely from undue influence, those legislative measures do fulfil a market-promoting function.[20] But they do so only instrumentally and at an aggregate level: primarily, they contrast Dark Patterns to restore fairness in an altered inter-individual transactional relationship.

New legislative measures on digital markets differ from earlier ones by focusing on the protection of *collective welfare*.[21] Both policies presented in the EU and the US mentioned above adopt a wider, market-oriented rationale for intervention, considering (also) the consequences of design practices on the entire digital economy and beyond.[22] The advent of the platform economy makes Dark Patterns associable with significantly higher risks and costs for society, going beyond the context of business-to-business (B2B) and business-to-consumer (B2C) practices.[23] A Dark Pattern may not only produce a benefit for the designer over users, but may also lead to objective harm.

We identify three collective welfare grounds for regulating Dark Patterns, which we explore closer within this paper.[24] First, some Dark Patterns may amount to so-called behavioural market failures[25]: producers use choice architecture designs that prey on systematically irrational behaviour of market participants, resulting in a distribution of welfare that is inefficient.[26] Second, Dark Patterns can undermine users' trust in digital markets and affect the credibility of companies who engage in fair practices.[27] Trust in digital markets may be severely diminished even if Dark Patterns are used by one single big firm.[28] Third, Dark Patterns may impair fair competition and reinforce data-opolies through data accumulation and misuse, two problems that privacy and data protection rules cannot remedy, just as antitrust rules also cannot.[29]

What explains the shift of focus from individual to collective welfare considerations are three factors that are new about Dark Patterns. First, their *granularity*: user experience design can be based on sophisticated algorithms,

[16]R. Van Loo, 'Broadening Consumer Law: Competition, Protection, and Distribution', (2019) 95 *Notre Dame Law Review*, 211 (contending that consumer law governs market transactions between individuals and companies implicating small instances of individual injustice).

[17]We intentionally do not employ expressions such as 'consumer welfare' and 'total welfare', because we are aware of the current debate surrounding their reframing, both in the economic and legal professions. For a great summary, see J. Padilla, 'Neoclassical Competition Policy Without Apology', (2022) *Working Paper*, retrievable at ssrn.com/abstract=4266176; L. Samuel and F. Scott Morton, 'What Economists Mean When They Say "Consumer Welfare Standard"', (2022) *Blogpost*, retrievable at https://www.promarket.org/2022/02/16/consumer-welfare-standard-antitrust-economists/.

[18]J.D. Wright, 'The Antitrust/Consumer Protection Paradox: Two Policies at War with Each Other', (2012) 121 *Yale Law Journal*, 2216, 2223, distinguishing between 'private' and 'social' welfare considerations in both antitrust and consumer law analyses.

[19]The mechanisms behind Dark Patterns have been discussed under the label of digital market manipulation for quite some time; see Calo, above, n. 11; Luguri and Strahilevitz, above, n. 3; L.H. Scholz, 'Private Rights of Action in Privacy Law', (2022) 63 *William & Mary Law Review*, 1639.

[20]This explains why the Unfair Commercial Practices Directive (UCPD), EU Directive 2005/29/EC, published in OJ L149/22, 11 May 2005, also explicitly aims to protect the competitive performance of markets by establishing a high level of consumer protection. For the US, see R. Van Loo, 'The Public Stakes of Consumer Law: The Environment, The Economy, Health, Disinformation, and Beyond', (2022) 107 *Minnesota Law Review*, 2039, 2085.

[21]See EU Dark Patterns Report (2022), above, n. 12, 120: 'Dark patterns and manipulative personalisation practices can lead to [individual welfare harm such as] financial harm, loss of autonomy and privacy, cognitive burdens, mental harm, as well as pose concerns for **collective welfare** due to detrimental effects on competition, price transparency and trust in the market' (emphasis added). Wright, above, n. 18.

[22]We use "collective welfare" to refer to constituting elements of welfare at the aggregate (i.e., market or society) level. This largely mirrors Wright's notion of 'social' welfare (Wright, above, n. 18).

[23]EU Dark Patterns Report (2022), above, n. 12, at 92; EDPB Guidelines (2022), above, n. 12, at 8–12.

[24]See Sections 3.1–3.3 below for greater detail.

[25]J.D. Hanson and D.A. Kysar, 'Taking Behavioralism Seriously', (1999), 74 *New York University Law Review*, 1425; O. Bar-Gill, 'The Behavioral Economics of Consumer Contracts', (2007) 92 *Minnesota Law Review*, 749, 792.

[26]See Section 3.1 below.

[27]Mathur et al., above, n. 6; Gray et al., above, n. 9; and M. Maier and R. Harr, 'Dark Patterns: An End-user Perspective', (2020) 16 *Human Technology*, 170.

[28]See Section 3.2 below.

[29]See Section 3.3 below.

TABLE 1 Grounds for regulating Dark Patterns

Individual welfare		Collective welfare	
Type of harm	**Regulation**	**Type of harm**	**Regulation**
Tricking users into consenting to their data processing	Privacy and data protection	Behavioural market failure	New digital market regulations *(US: AICO, DETOUR Act)* *(EU: DMA, DSA)*
Individual financial loss	Consumer protection *(US FTC Act, ROSCA, and other laws)* *(EU: GDPR, UCPD, CRD, UCTD)*	Loss of trust in markets	
Manipulating individual autonomy		Unfair competition/ reinforcement of data-opolies	
Goal: Preserving the ability of individuals to act in accordance with their preferences and maximise their welfare freely from undue influence of their counterparts		Goal: Correcting externalities that cannot possibly be adjusted at an individual level, or Adjusting digital market structure to account for Dark Patterns[a]	
Reason for the shift of focus: Granularity; Detail of behavioural observation; and Scale of Dark Patterns			

[a]This happens when individual-level policies could theoretically solve the problem of manipulation leading to no anticompetitive harm to remedy.

altering the appearance of a website based on personal characteristics of targeted individuals.[30] Secondly, the *detail* in which user behaviour can be observed is drastically improving in digital environments. This enables the design of websites in such a way that a certain user behaviour is promoted, down to even the smallest aspects.[31] Finally, and most importantly, the Dark Patterns employed by large digital platforms can reach millions of users, thus their impact has achieved a *scale* which was not possible before the advent of big digital players.

Against this backdrop, our contention is simple: solving the problem at the individual level doesn't sufficiently address the problem at the collective level. This is clear-cut where dark patterns create externalities: in such circumstances, a rational, non-manipulated user will still make decisions that are socially undesirable. Hence, we need policy that goes beyond correcting manipulation at the individual level.

The distinction between individual and collective welfare grounds is less stringent in one of the circumstances that we categorise as collective, such as the competition framework.[32] According to some, dark patterns can be theorised as an antitrust violation because they manipulate consumers into buying inferior products, short-circuiting competition.[33] However, while this theory could be useful as a way of getting antitrust enforcers to attack manipulative practices such as dark patterns, it falls short of providing a basis for arguing that individual-level initiatives would have been unable to solve the problem. Indeed, if policy were able to protect each user from manipulation at the individual level, then there would be no anticompetitive harm to remedy at the collective level—for then users would choose the products they prefer and firms offering those products would not be competitively handicapped in the market. In such a case, regulation can be better understood as a means aimed at adjusting market structures to account for dark patterns. Nonetheless, the theory is still valid if one considers the problem of data accumulation by big platforms, when (personal and non-personal) data is weaponised to exclude competition. Table 1 displays this assessment of differing regulatory rationales.

[30]For example, Netflix changes thumbnails of their content based on the observed user preferences: A. Chandrashekar et al., 'Artwork Personalization at Netflix', (2017) *Netflix Technology Blog*, retrievable at https://netflixtechblog.com/artwork-personalization-c589f074ad76.

[31]Anecdotally, Google conducted large-scale A/B testing comparing 41 shades of blue in order to determine which colour maximises the clickthrough rate for external advertisement links. The experiment, given the scale of Google's business, led to an increase of US$200 million a year in ad revenues. See A. Hern. 'Why Google has 200 m Reasons to Put Engineers over Designers', (2014) *The Guardian*, retrievable at https://www.theguardian.com/technology/2014/feb/05/why-google-engineers-designers.

[32]See Section 3.3 below.

[33]G. Day and A. Stemler, 'Infracompetitive Privacy', (2019)105 *Iowa Law Review*, 62.

Conceptualising digital manipulation as a collective welfare issue allows the tackling of the three concerns discussed above to be tackled in a direct and not instrumental fashion, thus enlarging the discussion over normative considerations. Under the new perspective, the employment of deceptive designs is tackled not in each and every case necessarily—such as happens under individual regulation cases—but only when they have a considerable impact on digital markets leading to broader societal harm.[34]

To go beyond individual user protection, the novel market-oriented regulations in the US (AICO and DETOUR Acts) and EU (DSA and DMA) establish a system of far-reaching protections both through the substantive content of the proposed regulations as well as their enforcement regimes. However, while the intentions of both legislators are commendable, this article will show that the proposed regulation only manages to achieve these goals to varying degrees of success. While the DMA provides substantial added protection for collective welfare by streamlining enforcement systems and targeting the key players in the market, the DSA, on the other hand—despite good intentions—only marginally improves the de facto level of protection. In the US, the DETOUR Act and AICO Act, if passed, would noticeably expand the scope of protection in favour of users.

Nonetheless, the collective welfare perspective highlighted here may also prove useful, in that it can be used to support a risk-based approach to the enforcement of existing laws and provide guidance as to which practices should be addressed with priority. Furthermore, those insights may help legislators amending existing laws to both achieve the said goals more consistently while streamlining the approaches used in the EU and the US.[35]

This article is organised as follows. First, in Section 2, we highlight the regulatory gaps of pre-existing laws in the EU and the US that address Dark Pattern practices from an individual welfare perspective. In Section 3, the collective welfare rationales for intervening on the use of Dark Patterns are discussed. We further examine the extent to which such rationales are conveyed in the European and US legislative proposals in Section 4. In Section 5, we assess those legislative measures and discuss their limitations showing that the collective-level goals are achieved to varying degrees. We then present the normative implications of the collective welfare approach in Section 6 by showing how these insights may enable a risk-based approach to be used by enforcing authorities in prioritising their activities and give guidance to legislators on how to enhance their legislative measures, Section 7 concludes.

2 | REGULATORY GAPS IN INDIVIDUAL-WELFARE LEGISLATION AGAINST DARK PATTERNS

Both the EU and the US already have mechanisms in place that effectively protect consumers from Dark Patterns. However, they come with considerable regulatory gaps. To briefly present the current scope of protection, Table 2 provides an overview of the practices which are most frequently identified as Dark Patterns, as well as their respective legal assessment in the EU and the US. For the EU, we distinguish between their implementation in a data protection context (DP), which is regulated by the General Data Protection Regulation (GDPR) regime,[36] and a consumer protection context (CP), considering the Unfair Commercial Practices Directive (UCPD), Unfair Contract Terms Directive (UCTD)[37] and Consumer Rights Directive (CRD).[38] For the US, no comparable granular system of regulations is in place. Instead, the Federal Trade Commission (FTC) handles Dark Patterns in both privacy and consumer protection cases as "unfair" or "deceptive practices" under Sect. 5 FTC Act.[39] While this makes it difficult to predict

[34]See Sections 3.1–3.3 below.
[35]See Section 4 below.
[36]General Data Protection Regulation (GDPR): EU Regulation 2016/679, published in OJ L119, 4 May 2016.
[37]Unfair Contract Terms Directive (UCTD): EU Directive 93/13/EEC, published in OJ L95, 21 April 1993.
[38]Consumer Rights Directive (CRD): EU Directive 2011/83/EU, published in OJ L304, 22 November 2011.
[39]FTC Act (15 U.S.C. § 45). Deceptive practices are—according to the FTC's definitional discretion (see *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233 (1972))—any 'presentation, omission, or practice' that is both important in consumer decision-making (materiality) and may potentially mislead reasonably acting consumers: FTC Policy Statement on Deception, 1984, 104 FTC 949.

TABLE 2 Individual welfare policies regulating Dark Patterns in the EU and US.

Name	Description	EU regulatory framework	U.S. case law
Sneak into Basket	Automatically adds products to the shopping cart (often labelled "bonus" or "necessary").	Consumer protection (CP): illegal, Art. 27 CRD.; Annex 1(29) UCPD Data protection (DP): does not apply	AH Media Group (19-CV-04022-JD); offering "free trials" and enrolling users in unwanted extensions
Hidden Costs	Discloses additional costs only shortly before the order process is completed. (e.g., "service fees").	CP: illegal, Art 6(1)(d), Art. 7(1), (4)(c) UCPD; Art. 6 (1)(e), Art. 22 CRD; Art. 4(2) Art. 5 UCTD DP: does not apply	No caselaw found, although effectively hiding cost-relevance information will likely fall under "deceptive acts", Sect. 5 FTC Act. See also FTC's ANPR on "drip prices" 2022
Hidden Subscription	Appearance shows one-time payment or free trial, but recurring payment obligation is established.	CP: illegal, Art. 6(1)(e), Art. 8(2) CRD; Art. 6(1)(b)(d), Art. 7 UCPD; Art. 3(3), Annex 1 h UCTD DP: does not apply	ABCmouse (2:20-cv-07996); not telling consumers that the plans would automatically renew. Amazon (Case 2:23-cv-00932)
Bait and Switch	Action performed results in a different outcome than expected (e.g., "x"-button on a pop-up window is not closing it but opening another website).	CP: potentially covered in very strong configurations, Art. 5 UCPD[a] DP: illegal in sufficiently pronounced cases, Art. 4 (11) GDPR (freely given, clear affirmation)	No caselaw found, although hiding cost-relevance information will likely fall under "deceptive acts", Sect. 5 FTC Act
Roach Motel	Choice design that makes it difficult to delete existing accounts or cancel subscriptions (e.g., by requiring unsubscribe emails).	CP: illegal in severe cases, Art. 8, Art. 9(d) UCPD or when employed to hide right to withdrawal Art. 6 (1)(h), Art. 10 CRD DP: illegal, Art. 7(3)(4) GDPR	ABCmouse (2:20-cv-07996); making it "*hard*" to cancel memberships (settlement over US $10 million and cessation of practices). Amazon (Case 2:23-cv-00932)
Bad Defaults	Preselection of the most invasive setting option as the default (e.g., preselection of optional insurance on e-commerce websites).	CP: illegal, when used for extending previous contracts Art. 22 CRD or inertia selling 27 CRD DP: illegal, Art. 4(11), Recital 32 GDPR (clear affirmation), Art. 25(1) GDPR	AMG Capital Management (16–17,197 (9th Cir. 2018)), preselecting a more expensive subscription plan. Amazon (Case 2:23-cv-00932)
Forced Subscription	Visiting a website/using a service is made possible only with setting up an account, that is technically unnecessary.	CP: potentially covered in strong configurations, Art. 8 UCPD DP: illegal, Art. 7(4) GDPR	Amazon (Case 2:23-cv-00932)
Urgency	Design elements suggesting special offers that are time-limited and will expire soon (e.g., countdown timers where expiration has no actual consequences).	CP: Illegal, if conclusion of a countdown bears no consequences, Annex I Nr. 7 UCPD DP: does not apply	See "Bait and Switch"

(Continues)

TABLE 2 (Continued)

Name	Description	EU regulatory framework	U.S. case law
Scarcity	Design elements suggesting high demand for a product/limited stock available.	CP: Illegal if limited availability is inaccurate, Annex I Nr. 7 UCPD. If scarcity throughout the market is implied, also Annex I Nr. 18 UCPD DP: does not apply	No caselaw found, although effectively hiding cost-relevant information will likely fall under "deceptive acts", Sect. 5 FTC Act
Social Proof	Messages suggesting fictional approval of the product/service by other buyers.	CP: Illegal if consumer reviews are not based on genuine experiences, Annex I Nr. 23b, 23c UCPD DP: does not apply	LeadClick Media (No. 15–1009 (2d Cir. 2016)), adding fake user-comments praising the product sold
Disguised Ad	Advertisements are integrated into the interface suggesting they are usable elements or content. When clicked, users are directed to an external website.	CP: Illegal if ad is hidden amongst search results, Annex I Nr. 11a UCPD or if commercial intent is undisclosed, Art. 7(2) UCPD DP: does not apply	LeadClick Media (No. 15–1009 (2d Cir. 2016)), designing ads to look like news articles
Visual Prominence	The workflow is influenced by the visual design of the user interface (e.g., some design elements are more visually appealing than others).	CP: legal, except for cases that effectively hide information, see "Hidden Information" DP: legal, except for cases that effectively hide information or when framing a consent decision as a "negative" option, Art. 4(11) GDPR	Commerce Planet, Inc. (09-CV-01324), using a blue font against a blue background. Amazon (Case 2:23-cv-00932)
Hidden Information	Certain elements, options or information is deliberately hidden (e.g., in sub-menus, fine print or visual design).	CP: illegal, if pre-contractual information, Art. 6, 8 II CRD; otherwise only illegal in pronounced cases, Art. 7(2) UCPD DP: illegal in pronounced cases, Art. 4(11) GDPR (fully informed)	*Progressive Leasing* (1:20-cv-01668); hiding material terms through auto-scroll features (company agreed to repay US$175 million to consumers). *AMG Capital Management* (16–17,197 (9th Cir. 2018)), hiding different payment options within a block of fine print. *Commerce Planet, Inc.* (09-CV-01324), using a blue font against a blue background. Amazon (Case 2:23-cv-00932)
Trick Questions	Deliberately misleading texts intended to overwhelm/confuse the user and lead her to make certain decisions (e.g., double negations).	CP: illegal in pronounced cases, Art. 6, 7 UCPD; Art. 4(2), 5 UCTD DP: renders consent invalid in pronounced cases, Art. 4(11) GDPR (clear affirmation, fully informed)	No caselaw found, although effectively hiding cost-relevant information will likely fall under "deceptive acts", Sect. 5 FTC Act

TABLE 2 (Continued)

Name	Description	EU regulatory framework	U.S. case law
Confirmshaming	Declining options are formulated as bad or irrational to elicit a negative emotional response (e.g., shame: "no, I do not want to save money").	CP: legal, might be covered by Art. 8, 9(b) UCPD in very pronounced cases DP: legal, except for very pronounced cases, Art. 4 (11) GDPR (freely given)	No caselaw found, although effectively hiding cost-relevant information will likely fall under "unfair acts", Sect. 5 FTC Act
Nagging	The task flow is interrupted by repeated requests (e.g., "Are you really sure" dialogue boxes) or repeated requests to consent to data processing are made.	CP: illegal in pronounced cases, Art. 8, 9(a) UCPD, Annex I Nr. 26 UCPD DP: illegal in pronounced cases, Art. 4(11) GDPR (freely given), Art. 25(1) GDPR	No caselaw found, although effectively hiding cost-relevant information will likely fall under "deceptive acts" or "unfair acts", Sect. 5 FTC Act
Click Fatigue	The task flow is complicated by making certain actions unnecessarily more strenuous, discouraging users from making those choices (e.g., unnecessary sub-menus).	CP: legal DP: legal	No caselaw found, although effectively hiding cost-relevant information will likely fall under "unfair acts", Sect. 5 FTC Act
Price Comparison Prevention	A user experience design that deliberately makes it difficult to compare prices with those of different vendors. For example, some e-commerce sites make the product information on their sites un-copyable to prevent users from comparing them with other sites.[b]	CP: legal DP: does not apply	No caselaw found, although effectively hiding cost-relevant information will likely fall under "deceptive acts" or "unfair acts", Sect. 5 FTC Act

[a]"Bait and Switch" should also include inviting customers to purchase a specific product at a—usually very low—price to generate their attention, but then refuse to sell it and instead promote a different product. See EU Dark Patterns Report (2022), above, n. 12, at 30, 32, 58, 64.
[b]EU Dark Patterns Report (2022), above, n. 12, 62. The British CMA qualifies "Drip Pricing" practices under this term as well (websites reveal the additional fees step by step, so that the overall price appears only at the end). Such practices, however resemble, a "Hidden Costs" pattern rather than a "Price Comparison Prevention".

the exact scope of Dark Patterns prohibited under US law, the precedents that have been established over the last few years are taken into account to provide such an overview.[40]

As Table 2 shows, both regulatory systems primarily focus on the prohibition of more aggressive cases of Dark Patterns. Smaller, more subliminal influences are not covered by either of the current regulatory frameworks. For example, less aggressive configurations of "Visual Prominence", "Nagging", "Trick Question" or "Click Fatigue" patterns have not been prohibited up to now. Designs that typically operate with more subtle emotional manipulation, such as "Confirmshaming" patterns, are essentially legal. This poses a considerable risk, as empirical evidence suggests that users are more susceptible to less aggressive designs.[41] Dark Patterns that are not particularly aggressive or conspicuous may thus ultimately exert a stronger influence on users' behaviour. In this regard, both jurisdictions show a systemic gap in user protection.

Additional to these material considerations, there are also problems at the enforcement level. This is the case in both jurisdictions. EU enforcement regimes allow consumers or advocacy groups to bring a claim, but remedies are often of limited effect, diluting overall deterrent potential.[42] Moreover, enforcement varies significantly between EU Member States due to differences in implementation of directives.[43] In the US, the FTC has pledged to combat transactional Dark Patterns that cause market-wide consumer harm.[44] However, the enforcement is limited in scope, overlooking unfair practices and privacy-focused Dark Patterns, and does not sufficiently address the prevalence of consumer harm in the marketplace. This appears contradictory as it recognises the widespread issue but provides limited solutions, underscoring a need for specific legislation targeting a broader range of Dark Patterns.

Ultimately, individual-level legislative measures are not well positioned to combat Dark Patterns, either because they are not capable of tackling all possible configurations (especially less severe instances) or because their enforcement by competent authorities and users is severely limited.

3 | COLLECTIVE WELFARE RATIONALES

For intervening against Dark Patterns, we identify three reasons that are based on collective welfare grounds,[45] and that individual-level initiatives cannot adequately tackle: behavioural market failures (Section 3.1), impairing market fairness (Section 3.2) and limiting fair competition and reinforcing data-opolies (Section 3.3). In the following, we analyse them separately.

3.1 | Behavioural market failures

From a neoclassical economic perspective, the intervention of the legislator in market activity requires justification, which is typically found in the existence of so-called market failure. If market failures occur, there is a suboptimal distribution of resources that cannot be resolved through market mechanisms.[46] The classic literature identifies four

[40]Most recently, the FTC has challenged several practices by Amazon under Sect. 5 FTC Act.

[41]Luguri and Strahilevitz, above, n. 3, 58–82, suggesting that users may be less capable to defend themselves as they do not notice the presence of a manipulation attempt.

[42]I. Graef, D. Clifford and P. Valcke, 'Fairness and Enforcement: Bridging Competition, Data Protection, and Consumer Law', (2018) 8 *International Data Privacy Law*, 200, 207; EU Dark Patterns Report (2022), above, n. 12, 122.

[43]See Art. 11 UCPD and Art. 11a UCPD.

[44]Federal Trade Commission, 'Enforcement Policy Statement Regarding Negative Option Marketing' (2021) 86 Fed. Reg 60,822. See also Federal Trade Commission, 'Staff Report "Bringing Dark Patterns to Light"', (2022a), *Workshop Proceedings*, retrievable at https://www.ftc.gov/reports/bringing-dark-patterns-light.

[45]See Table 1.

[46]F.M. Bator, 'The Anatomy of Market Failure', (1958) 72 *The Quarterly Journal of Economics*, 351, at 351–354.

types of market failures that justify intervention to increase social welfare: market power, externalities, public goods and informational asymmetries.[47]

Certain Dark Patterns convey information in an untransparent way and could already constitute information asymmetries.[48] However, many patterns function in a way that exploits behavioural biases, even if the information is provided. These may constitute a fifth category of market failures that has gained increasing recognition: behavioural market failures.[49] Such systematically irrational behaviour may also lead to inefficient outcomes, since producers use choice architectures that actively abuse irrational consumer behaviour, "sludging"[50] users into acting against their own preferences. As a result, consumer surplus may be transferred to the producer.[51]

Market mechanisms cannot solve this problem because competitors try to maximise the amount of feasible manipulation to reap the largest benefit from the market.[52] "Taking the high road" by not using manipulative designs does not grant a competitive advantage since this would require informing consumers about the existence and functionality of manipulative designs. And while informing consumers is potentially cost-intensive,[53] the implementing firm would not be able to enjoy the results, since competing firms can and will quickly dispose of their deceptive designs once consumer reaction to them becomes negative.[54]

Yet, it would be premature to ascribe all other Dark Patterns to behavioural market failures, since a market failure requires the transgression of a level of significance—some authorities also identify this to be precisely the threshold between individual and collective rationales for intervention.[55] Below this level of pertinence, frictions in the mechanisms of the market are to be considered *de minimis* and thus to be resolved by consumer protection law; only those issues that exceed this pertinence threshold are to be dealt with through regulation, which assumes a more collective perspective.[56] To surpass this threshold and constitute a demand-side failure, the behavioural influence on market mechanisms must be "substantial" and "sustainable".

A behavioural influence is "substantial" when welfare distribution deviates from the state of market equilibrium to a "non-negligible" degree, which is considered to be the case if firms obtain the power to significantly affect the overall market.[57] In principle, the use of Dark Patterns can have an impact of such degree on the market, given sufficient market power, as has already been recognised in the EU *Google Shopping* decision.[58]

This deviation from equilibrium outcomes is "sustainable" if users themselves cannot cope with their cognitive deviations and may not correct the behavioural shortcomings without external intervention.[59] It is true that the idea of self-correction cannot be fundamentally ruled out in the case of Dark Patterns—users become aware of certain methods and adapt their behaviour over the course of time.[60] However, digital platforms are able to create surroundings with exceptional manipulation abilities,[61] as they can quickly and frequently change their

[47]J. den Hertog, 'Economic Theories of Regulation', in R.J. van den Bergh and A.M. Pacces (eds.), *Regulation and Economics* (Edward Elgar, 2012), 25.

[48]For example: "Disguised Ad", "Hidden Information", "Trick Question" or "Price Comparison Prevention" patterns.

[49]Hanson and Kysar, above, n. 25; O. Bar-Gill, 'Consumer Transactions', in E. Zamir and D. Teichman (eds.), *The Oxford Handbook of Behavioral Economics and the Law* (Oxford University Press, 2014), 465, 477–486.

[50]R. Thaler, 'Nudge, not Sludge', (2018) 6401 *Science*, 1.

[51]O. Bar-Gill, above, n. 49, 477–486.

[52]M.R. Leiser, '"Dark Patterns"': The Case of Regulatory Pluralism', in E. Kosta et al. (eds.) *Research Handbook on EU Data Protection Law* (Edward Elgard, 2022), 240, 241 f.

[53]K. Bongard-Blanchy et al., '"I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous!"—Dark Patterns from the End-User Perspective', (2021) *Designing Interactive Systems Conference Proceedings*, retrievable at https://doi.org/10.1145/3461778.3462086.

[54]O. Bar-Gill, above, n. 49, 475 ff.

[55]P. O'Loughlin, 'Cognitive Foreclosure', (2022) 38 *Georgia State Law Review*, 1166.

[56]Different from our proposal, O'Laughlin, ibid., 1167 suggests that behavioural market failures (stemming from Dark Patterns) may be resolved through antitrust enforcement.

[57]G. Colangelo and M. Maggiolino, 'Manipulation of Information as Antitrust Infringement', (2019) 26 *Columbia Journal of European Law*, 90.

[58]EU Court of Justice (Grand Chamber), Case T-612/17, *Google LLC & Alphabet, Inc. v. Commission* (*Google Shopping*), 10 November 2021, T:2021:763. The Commission's decision is Case AT.39740, *Google Search (shopping)*, 27 June 2017. Both find that the influence on the display form of the placement on a search engine page has a significant impact on the traffic of the respective website.

[59]O'Loughlin, above, n. 55, 1169.

[60]D.C. Langevoort, 'Behavioral Theories of Judgment and Decision Making in Legal Scholarship: A Literature Review', (2998), 51 *Vanderbilt Law Review*, 1499, 1521.

[61]O'Loughlin, above, n. 55, 1123–1143 provides an extensive explanation of this.

interface design and adapt it to other behavioural imperfections if they notice that certain techniques are becoming less effective—an event that is unlikely to escape their attention because of extensive A/B testing.[62] In addition, empirical results suggest that less prominent Dark Patterns still influence behaviour but are much less likely to be recognised by users, making it less probable that they will adapt their behaviour to counter less aggressive design techniques.[63]

The preceding illustrates that Dark Patterns are indeed capable of substantially and sustainably influencing market mechanisms and can therefore warrant intervention on the basis of collective welfare reasoning. As a result of behavioural market failures, Dark Patterns may therefore be a relevant object of regulation. In this context, however, the economic power of the website which employs Dark Patterns must be taken into account, as the impact of individual interface designs depends strongly on the reach and influence of the website in question. Through this channel, the regulation of Dark Patterns aims not only to protect individuals but also to promote collective welfare for all market participants.

3.2 | Trust in markets

A second collective welfare account for intervening is trust in markets. Dark Patterns can undermine users' trust in digital markets and affect the credibility of companies who engage in fair practices.[64] Although several Dark Patterns are unfair and illegal under existing consumer protection laws, this occurs mainly on a case-by-case basis, after assessing the individual contextual framework where they occur.[65] Individual-level provisions and decisions by competent authorities could allow for the accumulation of knowledge about which design practices are effectively illegal, but they are effectually limited, resulting in considerable leeway for firms when it comes to interface design. This leads to the widespread use of Dark Patterns as a common market practice, which weakens trust of users in digital markets.[66]

When asymmetric information generated through Dark Patterns creates widespread distrust, regulation is justified[67] to make the bridge of online intermediaries and their users effective.[68] The trust-in-market rationale has a wider reach than has the lack of information in individual transactional relationships. In the latter, the consideration given to platforms' behaviour is purely instrumental to the achievement of the welfare of users.[69] The reason to contrast Dark Patterns in consumer protection rules is primarily one of restoring fairness in the altered interindividual transactional relationship, and only indirectly to have a functioning market. However, once the reach of Dark Patterns is so pervasive to have an impact that is unavoidable, then markets cannot function properly. And this failure needs to be tackled.

Finally, a collective action problem may arise. Even if individual costs associated with Dark Patterns are minimal, the aggregate level might still significantly impact collective welfare.[70] This in turn raises a social dilemma regarding the prosecution of Dark Patterns, given that under the current enforcement system, the costs are mostly borne by

[62]A/B testing is a research methodology used to compare and evaluate the effectiveness of two different versions of a single variable—commonly an element of a digital user interface. Users are randomly assigned to one of two groups, the performance of which are then compared based on predefined metrics, such as clickthrough rates or conversion rates. See more under Section 5.2.1.1).

[63]Bongard-Blanchy et al., above, n. 53.

[64]Maier and Harr, above, n. 27, 170–199; see also Mathur et al., above, n. 6; Gray et al., above, n. 9.

[65]K. Bania, 'Fitting the Digital Markets Act in the Existing Legal Framework: the Myth of the "Without Prejudice" Clause', (2023), 19 *European Competition Journal*, 116, 127.

[66]Dark Patterns may let users overestimate the level of protection legal systems grant to their privacy and security rights, making them trust digital intermediaries based on mistaken assumptions: Luguri and Strahilevitz, above, n. 3.

[67]T. Rodríguez de las Heras Ballell, 'The Background of the Digital Services Act: Looking towards a Platform Economy', (2021) 22 *ERA Forum*, 75.

[68]A. Turillazzi, M. Taddeo, L. Floridi and F. Casolari, 'The Digital Services Act: An Analysis of its Ethical, Legal, and Social Implications', (2022) 15 *Law Innovation and Technology*, 8, 12.

[69]F. Esposito, *The Consumer Welfare Hypothesis in Law and Economics: Towards a Synthesis for the 21st Century* (Edward Elgar, 2022).

[70]EU Dark Patterns Report (2022), above, n. 12, at 122.

individual users, while the benefits are public.[71] Dark Patterns can thus be understood as a collective action problem[72]: challenging deceptive interfaces in court can be costly and time consuming, since consumers or the associations representing their interests would carry the burden of proof. Similarly, high amounts of legal uncertainty and costs will prevent firms from bringing these actions against their competitors. Thus, regulation of Dark Patterns may be justified to establish public enforcement in well-identified and particularly harmful cases.

The trust in market rationale transcends B2C relationships, because in digital ecosystems, traders may be exposed to the same vulnerabilities and costs of individual consumers. However, because traders are also often competitors of digital platforms, we will discuss how Dark Patterns might affect platform-to-business (P2B) relationships in the analysis of the third collective welfare rationale, which is devoted to competition concerns.

3.3 | Promoting fair competition and combating data-opolies

A third underexplored collective welfare rationale for combating Dark Patterns concerns their impact on competition in digital markets. In highly concentrated markets, like most digital ones,[73] the options available to users are very limited (if existent at all), often being dependent on a few big providers which may easily engage in unfair practices. For instance, a "Roach Motel" pattern employed by a gateway platform that reaches millions of end users could induce an enormous number of them to believe that easily unsubscribing from a service is not possible, preventing them from changing to competitors or more innovative firms. This scenario is different from the one consumer laws commonly tackle,[74] because the collective harm of one single Dark Pattern may be significantly higher, given the considerable number of users.

Dominant gatekeeper platforms control not only the consumption of services and goods by their own users, but also access of traders to end consumers. At the same time, they 'play a dual role, being simultaneously operators for the marketplace and sellers of their own products and services in competition with rival sellers'.[75] Dark Patterns may be used to cumulate data, or force users into contracting with digital platforms to extend their economic power in new markets (e.g., through tying-in unrelated products), or keep users in their walled gardens (e.g., by heightening switching costs).

Attempts to configure Dark Patterns as an antitrust infringement have previously been made.[76] For instance, Day and Stemler use precedents of coercion by US courts,[77] to assert that Dark Patterns may harm competition. That is because they 'coerce users into spending attention, generating data, and paying money without doing so on the merits',[78] thus having exclusionary effects leading to market failures. Especially, they hook users to a platform while erecting barriers to entry and hamper switching where better alternatives are present. Thus, antitrust scrutiny would be justified to remedy such failure, but only if the pattern was meant to 'enhance addiction and manipulate usage while providing consumers with a qualitatively worse product'.[79]

[71]EU Dark Patterns Report (2022), above, n. 12, at 122.

[72]M. Olson, *The Logic of Collective Action* (Harvard University Press, 1971).

[73]G. Colangelo, 'Evaluating the Case for Regulation of Digital Platforms', (2020) *The Global Antitrust Institute Report on the Digital Economy 26*, retrievable at https://ssrn.com/abstract=3733741, 1. See, also, Rodríguez de las Heras Ballell, above, n. 67, 80.

[74]See Van Loo, above, n. 16, 211, suggesting that the traditional vision of consumer law as governing market transactions between people and companies should be abandoned to embrace a more holistic consumer law, capable of also promoting public goods such as fostering health, protecting the environment, combating misinformation.

[75]Colangelo, above, n. 73, 1.

[76]O'Loughlin, above, n. 55, configuring Dark Patterns as a new form of demand-side behavioural market failure (so-called "cognitive foreclosure"), that may attract antitrust scrutiny; see also Day and Stemler, above, n. 33, 34.

[77]Day and Stemler, above, n. 33. Microsoft's use of a default interface was found to be anticompetitive by the D.C. Circuit Court as it overrides the preferences of consumers in forcing them to use Internet Explorer, even if it is of an inferior quality than other browsers. *United States v. Microsoft Corp*., 253 F.3d 34, 65 (D.C. Cir. 2001).

[78]Day and Stemler, above, n. 33, 34.

[79]Ibid., 35.

Although useful in the antitrust realm, this theory does not provide full basis for arguing that individual-level initiatives would be unable to tackle the issue. Theoretically, if those policies were able to protect each user from manipulation at the individual level, then there would be no anticompetitive harm to remedy at the collective level, because users would choose the preferred alternatives and firms offering those products would not be competitively handicapped in the market. Hence, this antitrust theory could apply only where no substitutes are present. But if those (worse) alternatives existed, this theory would lead to enforcement difficulties: if providing evidence of a qualitatively worse product may be easy, a wide range of problems are attached to the demonstration of enhancing addiction. Moreover, the design or re-design of an interface is considered (by US courts) to be an act of innovation and should be not only permitted but encouraged.[80] Thus, it could be hard to prove that an interface element constitutes a Dark Pattern in the first place, unless ex-ante regulation states so.

Concerning the remedies, one would need to assess the implications for consumer surplus and (total) welfare of a ban on Dark Patterns. In this regard, not much research has been conducted, because Dark Patterns themselves are not yet considered an antitrust infringement as such. However, Hagiu, Teh and Wright[81] provide evidence of welfare implications of different remedies to self-preferencing performed through Dark Patterns[82] by dominant platforms acting in dual mode. They demonstrate that imposing a (behavioural) ban on both imitation (or the possibility for the platform to copy third-party sellers' innovations) and visual prominence patterns would increase total welfare.[83] That is because a ban on imitation would 'restore the sellers' incentive to innovate', whereas a ban on prominence would restore effective price competition between products or prevent 'the platform from extracting excessively high commissions from third-party sellers'.[84] Even if remedial hurdles do not seem insurmountable, it may still be hard to prove that the expected costs of intervening against Dark Patterns as such and not the entire self-preferencing strategy (Type I errors) are smaller than those of no intervention (Type II errors).

Another argument to justify intervention against Dark Patterns from a collective welfare perspective concerns data accumulation.[85] From a supply-side perspective, Dark Patterns can ease data accumulation by big tech firms or data-opolies[86]—yet another, more contested, competition concern.[87] Since data is the main input of the platform economy, collection and analysis of enormous amounts of personal and non-personal data may be weaponised to exclude competition. Several competition authorities around the world,[88] as well as data protection authorities,[89] have raised this concern. Big platforms use data to deliver targeted advertising, personalise services, and enhance synergies between their brands and business partners. That is why accumulating users' personal and non-personal data is so essential and why Dark Patterns may be an easy tool to achieve this goal.

[80]The idea that changes in product design by a dominant firm do not trigger per se competition concerns has been repeatedly remarked in the US case law. See Berkey *Photo, Inc. v. Eastman Kodak Co*., 603 F.2d 263, 281 (2d Cir. 1979); *United States v. Microsoft Corp*., 253 F.3d 34, 65 (D.C. Cir. 2001).

[81]A. Hagiu, T.H. Teh and J. Wright. 'Should Platforms Be Allowed to Sell on their own Marketplaces?', (2022) 53 *The RAND Journal of Economics*, 297.

[82]The authors analyse the effects of self-preferencing enacted, inter alia, through "Visual Prominence" patterns, which allows consumers to be steered to buy from the platform itself.

[83]Hagiu et al., above, n. 81, 320.

[84]*Ibid*.

[85]FTC (2022a), above, n. 44.

[86]M.E. Stucke, 'Should We Be Concerned About Data-Opolies?', (2018) 2 *Georgetown Law Technology Review*, 275.

[87]The number of antitrust scholars who have written about the interplay between privacy/data protection and competition law is enormous. To name a few: C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown Publishing Group, 2016); A. Witt, 'Data, Privacy and Competition Law', (2021) *Graz Law Working Paper No. 24–2021*, retrievable at https://ssrn.com/abstract=3989241.

[88]E.g., the DOJ Antitrust Division—see M. Delrahim, '"Blind[ing] Me With Science": Antitrust, Data, and Digital Markets', (2019) *Policy Statement*, retrievable at https://www.justice.gov/opa/speech/file/1217071/download); the European Commission—see Commissioner M. Vestager, '"Competition in a Big Data World"', (2016) *Speech at the DLD Conference, Munich, 17 January 2016*, video available at https://www.youtube.com/watch?v=I3eb036cYNY); the German Bundeskartellamt—see Bundeskartellamt, 'Bundeskartellamt prohibits Facebook from combining user data from different sources', (2019) *Press Release from 7.2.2019*, retrievable at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html); and the Italian Competition Authority—see AGCM-AGCOM-Garante, 'Privacy, Indagine conoscitiva congiunta su big data', (2020) *Press Release from 10.02.2020*, retrievable at https://www.agcm.it/media/comunicati-stampa/2020/2/Big-Data-pubblicata-indagine-Agcom-Agcm-e-Garante-privacy).

[89]European Data Protection Supervisor (EDPS), 'Opinion 2/2021 on the Proposal for a Digital Markets Act', *Policy Statement*, 10.02.2021.

Data protection legislative measures that could potentially protect individuals against mass collection and misuse of data do exist. However, these legislative measures are not necessarily the right tool to counteract Dark Patterns. First, they usually pertain only to personal data and do not cover inferred and derived data. However, Dark Patterns can be used to collect both (non-personal) traders' data, and inferred and derived data (like profiles that are created by data controllers). Second, data protection regimes do not aim to protect competition, even if digital markets are fuelled by data, because competition reflects interests beyond the protection of individual privacy consent.

Finally, users' consent cannot be employed to keep markets contestable because privacy laws protect individuals' rights based on individual consent, but the latter cannot prevent competitive harm, due to data externalities.[90] Data combination by large tech companies works in such a way that if one or more users consent to their data being exchanged among different services (of the same or different companies), this choice affects users belonging to the same category, even if they have not expressed their consent. The consent obtained through Dark Patterns will provide insights also on users showing similar preferences or behavioural characteristics.[91] It follows that outlawing Dark Patterns based on data protection regimes can hardly succeed in tackling collective competitive harm and externalities.[92] For this reason, regulation that tackles data combination through Dark Patterns could be justified beyond reference to individual consent.[93]

4 | COLLECTIVE WELFARE POLICIES: EU AND US COMPARED

To illustrate how the collective welfare grounds are conveyed into the new policy initiatives, we analyse the content of new market-oriented legislative measures and categorise them with regard to their goals. First, we consider legislation aimed at restoring trust in markets and promoting fairness in markets, namely: the European DSA and the American DETOUR Act (Section 4.1). Then, we turn towards those legislative endeavours aimed at regulating big tech to enhance competition, namely the European DMA and the proposed AICO Act in the US (Section 4.2). Table 3 offers a tabulated overview of our results.

4.1 | Digital Services Act (DSA) and DETOUR Act: tackling behavioural market failures and restoring trust in digital markets

4.1.1 | The DSA

The DSA addresses online intermediary services offered to users in the EU by setting duties of care and liability requirements in a graded, incremental regulatory fashion: all intermediary services are subject to general obligations, which are supplemented by additional stricter obligations depending on the type and size of intermediary. The strictest requirements are imposed on very large online platforms (VLOPs) and very large online search engines (VLOSEs).[94]

The main provision regulating Dark Patterns is Art. 25 DSA, where para. (1) prohibits online platforms[95] and the VLOPs and VLOSEs, to 'design, organise or operate […] online interfaces in a way that deceives or manipulates […]

[90] I. Graef, 'Why End-User Consent Cannot Keep Markets Contestable', in H. Richter, M. Straub and E. Tuchtfeld (eds.), *To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package* (Max Planck Institute for Innovation and Competition Research Paper Series, 2021), No. 21–25, 78. See also G. Malgieri and A. Davola, 'Data-Powerful', (2022) *Working Paper*, retrievable at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4027370.

[91] J. Fairfield and C. Engel, 'Privacy as a Public Good', (2015) 65 *Duke Law Journal*, 385, 399 ff., 423 f.

[92] Graef, above, n. 90.

[93] Ibid.

[94] From here on we refer only to VLOPs for brevity, but all considerations made can be extended to VLOSEs.

[95] Art. 3(i) and Recital 14 DSA.

TABLE 3 Collective welfare policies regulating Dark Patterns in the EU and U.S.

Name	DMA and DSA	Proposed DETOUR and AICO Acts
Sneak into Basket	25(1) DSA: potentially covered as an interface design that materially distorts users' behaviour. Further details may be defined in Commission guidance.	3(a)(1) DETOUR Act: practice could obscure/subvert user choice or decision-making; potentially prohibited if used to obtain consent (practice not used for data gathering).
Hidden Costs	25(1) DSA [see Sneak into Basket]	3(a)(1) DETOUR Act: [see Sneak into Basket]
Hidden Subscription	25(1) DSA: [see Sneak into Basket]	3(a)(1) DETOUR Act: [see Sneak into Basket]
Bait and Switch	25(1) DSA: [see Sneak into Basket]	3(a)(1) DETOUR Act: [see Sneak into Basket]
Roach Motel	6(13) DMA (GK cannot establish disproportionate conditions for terminating provision of CPS and must ensure **termination** be exercised without **undue difficulty**). 13(4) + 5(2)(d) DMA (making difficult to delete Forced Subscription, which is illegal, thus remaining with existing provider) 25(3)(c) DSA "making the procedure for terminating a service more difficult than subscribing to it".	AICO Act: (no equivalent). DETOUR Act: (no equivalent; does not apply, since practice is not used to obtain consent or user data).
Bad Defaults	6(3) DMA (GK to allow **end users** to 'easily change' the default settings on their operating systems, virtual assistants and web browser that 'direct' or 'steer' **end users** to the products or services that they provide). 25(1) DSA: [see Sneak into Basket] see Recital 67 (2) DSA.	2(b)(5) **AICO Act** covered platforms cannot "materially restrict or impede covered platform **users** from uninstalling software applications that have been preinstalled on the covered platform or changing default settings that direct or steer covered platform users to products or services offered by the covered platform operator". 3(a)(1) DETOUR Act: [see Sneak into Basket]
Forced Subscription	5(2)(d) DMA (GK shall not sign-in end users to other services of the GK in order to combine personal data). 5(8) DMA (GK shall not require users to subscribe or register with other CPSs as a condition of access to another CPS operated by the same gatekeeper). 25(1) DSA: [see Sneak into Basket]	AICO Act: (no equivalent). 2(b)2 **AICO Act** (covered platforms cannot condition access to the covered platform or preferred status or placement on the covered platform on the purchase or use of other products or services offered by the covered platform operator). 3(a)(1) DETOUR Act: [see Sneak into Basket]
Urgency	13(4) + 6(3) DMA using Urgency to impede to 'Easily change the default settings', that is illegal. 25(1) DSA: [see Sneak into Basket]	3(a)(1) DETOUR Act: [see Sneak into Basket]
Scarcity	13(4) + 6(3) DMA using Scarcity to impede to 'Easily change the default settings', that is illegal. 25(1) DSA: [see Sneak into Basket]	3(a)(1) DETOUR Act: [see Sneak into Basket]
Social Proof	25(1) DSA: [see Sneak into Basket]	3(a)(1) DETOUR Act: [see Sneak into Basket]
Disguised Ad	25(1) DSA: [see Sneak into Basket]	3(a)(1) DETOUR Act: [see Sneak into Basket]
Visual Prominence	13(6) + 6(5) DMA using Visual Prominence to circumvent self-preferencing prohibition.	3(a)(1) DETOUR Act: [see Sneak into Basket]

TABLE 3 (Continued)

Name	DMA and DSA	Proposed DETOUR and AICO Acts
	25(3)(a) DSA: 'giving more prominence to certain choices when asking the recipient of the service for a decision'	
Hidden Information	25(1) DSA: [see Sneak into Basket]	3(a)(1) DETOUR Act: [see Sneak into Basket]
Trick Questions	25(1) DSA: [see Sneak into Basket]	3(a)(1) DETOUR Act: [see Sneak into Basket]
Nagging	5(2)(d) last part[a] DMA (If consent to data processing was refused or withdrawn by the end users, GK cannot repeat the request for the same purpose more than once per year + to avoid Forced Subscription). 25(3)(b) DSA 'repeatedly requesting that the recipient of the service make a choice where that choice has already been made, especially by presenting pop-ups that interfere with the user experience'	AICO Act: (no equivalent). 3(a)(1) DETOUR Act: [see Sneak into Basket]
Click Fatigue	6(13) DMA (GK cannot establish disproportionate conditions for terminating provision of CPS and must ensure termination be exercised **without undue difficulty**). 25(1) DSA: [see Sneak into Basket], see Recital 67 (2) DSA.	AICO Act: (no equivalent). 3(a)(1) DETOUR Act: [see Sneak into Basket]
Confirmshaming	6(13) DMA (GK cannot establish disproportionate conditions for terminating provision of CPS and must ensure termination be exercised **without undue difficulty**). 25(1) DSA: [see Sneak into Basket]	AICO Act: (no equivalent). 3(a)(1) DETOUR Act: [see Sneak into Basket]
Price Comparison Prevention	25(1) DSA: [see Sneak into Basket]	3(a)(1) DETOUR Act: [see Sneak into Basket]

[a]Art. 5(2) DMA last part: Gatekeepers can, nonetheless, utilise other legal bases to process personal data of end users.

or [...] otherwise materially distorts or impairs the ability of the recipients of [the] service to make free and informed decisions'.[96]

Art. 25 DSA only applies to platforms that are at least of medium size,[97] and to VLOPs. Essentially that means that Dark Patterns are problematic only if implemented by firms that have a meaningful presence in the EU market. As a result, not all Dark Patterns are regulated, but only those that may have a significant impact, in line with the collective welfare rationale outlined above.

Art. 25(3) DSA further gives an exemplificatory list of Dark Patterns on which the Commission should provide guidance, implying that the activities defined therein surely qualify as Dark Patterns. These are: "Visual Prominence", "Nagging" and "Roach Motel" patterns.[98]

[96]While the article does not explicitly mention Dark Patterns, the conduct prohibited by Art. 25(1) DSA aligns almost perfectly with the definition of Dark Patters provided in Recital 67 DSA.

[97]Art. 29(1) DSA excludes applicability for micro and small enterprises as defined in Recommendation 2003/361/EC, i.e., enterprises which have less than 50 employees and whose annual turnover does not exceed €10 million.

[98]Art. 25(3)(a), (b) and (c) DSA, respectively.

4.1.2 | The proposed DETOUR Act

The proposed DETOUR Act aims to impose a comprehensive set of obligations on large online operators, which are defined as any entity providing an online service[99] which has more than 100,000,000 authenticated users in a 30-day period and is subject to the jurisdiction of the FTC. It prohibits those operators 'to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data'.[100] Like Art. 25 DSA, the provision is broadly worded and does not address specific design practices, but instead refers to the underlying mechanism of influencing user behaviour and autonomy through design. Thus, it works as a suitable general clause to cover an absolute majority of Dark Patterns. Like in the DSA, the term Dark Patterns is not explicitly mentioned, but it is clear from the accompanying material that this is an explicit objective of the proposal.[101] Any breach of the DETOUR Act[102] is enforced by the FTC as a violation of a rule defining unfair or deceptive practices,[103] and the FTC enjoys the enforcement powers under the FTC Act as well as the ability to establish guidelines.[104]

4.2 | Digital Markets Act (DMA) and AICO Act: tackling unfair competition and limiting data-opolies

4.2.1 | The DMA

The DMA is a competition-oriented piece of regulation which aims to foster fairness and contestability of digital markets where dominant players operate. Similarly to the DETOUR Act and (to some extent) DSA, it applies only to big platforms that are designated as gatekeepers[105] in relation to core platform services (CPS).[106] Gatekeepers are subject to a wide range of ex ante obligations and prohibitions that that are either self-executing (Art. 5 DMA) or require further specification by the Commission through implementing acts (Art. 6 DMA).

Although the DMA does not mention Dark Patterns expressly, they are nonetheless regulated in two ways: either (a) they are prohibited as such; or (b) they are made illegal if used to circumvent other duties established by the DMA.

Dark Patterns prohibited as such

Art. 5(2)(d) DMA makes "Forced Subscription" illegal by preventing gatekeepers from signing-in end users to access different services.[107] "Forced Subscription" patterns are illegal also under Art. 5(8) DMA, whereby gatekeepers cannot require users to subscribe or register with other CPSs as a condition of access to another CPS operated by the same gatekeeper. "Nagging" patterns to gather consent to data treatment are prohibited too, since the last part of

[99]Sect. 3(a)(1) and Sect. 2(8) DETOUR Act.

[100]Sect. 3(a)(1) DETOUR Act.

[101]See Senator M. Warner, 'Lawmakers Reintroduce Bipartisan Bicameral Legislation to Ban Manipulative "Dark Patterns"', (2021) *Press Release from 08.12.2021*, retrievable at https://www.warner.senate.gov/public/index.cfm/2021/12/lawmakers-reintroduce-bipartisan-bicameral-legislation-to-ban-manipulative-dark-patterns.

[102]This applies also to other duties laid down in Sect. 3(a) or (b) DETOUR Act. For example, Sect. 3(a)(3) and Sect. 3(b)(5)(6) DETOUR Act.

[103]Sect. 3 (d)(1)(A) DETOUR Act.

[104]Sec. 3(d), DETOUR Act: violations of its obligations are to be considered violations of rules defining unfair or deceptive acts or practices under Sect. 5 FTC Act. Guidelines for rules for obtaining the informed consent of users, for independent review boards and professional standards bodies may be issued according to Sect. (c)(2) DETOUR Act.

[105]To be designated, gatekeepers must pass a three-tier test based on qualitative criteria (Art. 3(1) DMA). Quantitative thresholds are established, meeting which implies (a rebuttable presumption) that each tier is met (Art. 3(2) DMA). If the quantitative thresholds are not met, the Commission may nonetheless designate a company as a gatekeeper following a market investigation under Art. 17, Art. 3(8) DMA.

[106]Art. 17 DMA.

[107]Unless they are presented with a specific choice and have given explicit consent under the meaning of Art. 4(11) DMA and Art. 7 GDPR.

Art. 5(2) DMA forbids gatekeepers from reiterating consent requests more than once per year, if the consent was refused or withdrawn by end users.[108]

Other Dark Pattern are made illegal under Art. 6 DMA, which implies that more guidance will be provided in due course by the Commission. "Bad Default" patterns would be illegal under Art. 6(3) DMA, which obliges gatekeepers to allow end users to 'easily change' the default settings on their operating systems, virtual assistants and web browser, if the default 'directs' or 'steers' end users to the products or services that they provide.[109] Directing or steering end users by default is seen as especially problematic if performed at the time of first use of an online search engine, virtual assistant, or web browser of the gatekeeper.[110] Lastly, Art. 6(3) DMA would make "Roach Motel"—but also more subtle techniques such as "Click Fatigue" and "Confirmshaming" patterns—illegal, if gatekeepers do not ensure (in their terms and conditions) that terminating the provision of a CPS is exercised without undue difficulty and in a proportionate way.

Dark Patterns made illegal if used for circumvention purposes (Art. 13 DMA)

Under Art. 13 DMA, Dark Patterns are not prohibited as such but are instead considered means to circumventing the substantial duties set out in the DMA. Specifically, Art. 13(4) DMA prevents gatekeepers from violating the "dos" and "don'ts" they are subject to through the use of 'behavioural techniques or interface design'. Those interfaces shall not be designed, organised, or operated in ways that deceive, manipulate or otherwise materially distort or impair the ability of end users to freely give consent.[111] To capture the potential of Art. 13(4) DMA, one needs to read it in conjunction with each individual misconduct identified in Art. 5 DMA[112] and Art. 6 DMA.[113]

An example of Dark Patterns that could be caught thanks to the 'scope-widening' force of Art. 13 DMA is "Roach Motel". Circumventing Art. 5(2)(d) DMA ("Bad-Default" patterns), may be done through "Forced Subscription". That means that, if a "Forced Subscription" situation is not caught in the first instance (by Art. 5(2)(d) DMA), the same goal of preventing end users from sticking may be attained by forbidding "Roach Motel" patterns, which impede end users exercising their free choice to opt out from data processing.

In a similar way, Art. 13(6) DMA also has a liability-widening function, given that it prevents gatekeepers from circumventing their duties by 'subvert[ing] end users' or business users' autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface or a part thereof'. To avoid this, the provision requires gatekeepers to design their interface and present choices 'in a neutral manner'.[114]

[108]An exception is possible although in very limited cases.

[109]Prior to the DMA's adoption, "Bad Default" patterns by Facebook were found unfair by the Italian Competition Authority (29 November 2018), which fined Facebook €10 million for (i) preselecting the broadest possible consent to data sharing, and (ii) preselecting defaults that enabled the transmission of personal data to single websites/apps without any express consent. See also Court of Justice (Grand Chamber), 1 October 2019, C-673/17 *Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH*, ECLI:EU:C:2019:801.

[110]For this reason, gatekeepers are bound to allow end users to choose 'from a list of the main available service providers, the online search engine, virtual assistant or web browser to which the operating system of the gatekeeper *directs* or *steers* users by default, Art. 6(3) DMA (emphasis added).

[111]Recital 36 DMA.

[112]Don'ts include: processing (Art. 5 (2)(a) DMA), combining (*lit*. b) or cross-using (*lit*. c) personal data of end users across CPS or between CPS and other services or to sign in end users (*lit*. d) to other services without the end user's consent (Bundeskartellamt, Case B6–22/16, *Facebook*, 6 February 2019); making use of Most-Favoured Nation clauses (Art. 5 (3) DMA (see EC Case AT.40153, *E-book MFNs and Related Matters (Amazon)*, 4 May 2017)); limiting users' legal remedies (Art. 5 (6) DMA); tying (Art. 5 (7) DMA); requiring users to subscribe or register with other CPSs as a condition of access to another CPS operated by the same gatekeeper (Art. 5 (8) DMA see EC, Case AT.40099, *Google Android*, 18 July 2018). The dos include: allowing communication to end users free of charge (Art. 5 (4) DMA); allowing end users to access and use content, subscriptions, features or other items by using business parties' service applications (Art. 5 (5) DMA); providing advertising customers with information on advertising prices (Art. 5 (9) DMA); giving publishers information on advertising prices (Art. 5 (10) DMA, EC, Case AT.40670, *Google - AdTech and Data Related Practices*, 22.6.2021).

[113]Dos include to: allow end users to un-install preinstalled software applications and change default settings (Art. 6(3) DMA); permit end users to sideload (i.e. installing apps) of business users (Art. 6(4) DMA); allow vertical interoperability (i.e. not giving preferential access to hardware, operating system, software features to their own complementary and supporting services) (Art. 6(7) DMA); provide advertisers and publishers with access to performance measurement tools (Art. 6(8) DMA); grant end users access to CPS data (Art. 6(9) DMA); grant business users and authorised third parties access to CPS data (Art. 6(10) DMA); provide search engines with access to search data on FRAND terms (Art. 6(11) DMA); grant business users with access to app stores, search engines and social networks on FRAND terms (Art. 6(12) DMA). Conduct that is prohibited under Art. 6 DMA include: Sherlocking (or using business users' data to compete against them) (Art. 6(2) DMA (EC, Cases AT.40462, *Amazon Marketplace*; 10.11.2020, and AT.40684, *Facebook leveraging* 4.6.2021); self-preferencing in ranking, indexing and crawling (Art. 6(5) DMA (EC *Google Search (shopping)*, above, n. 60); limiting switching (Art. 6(6) DMA); applying disproportionate conditions to terminate CPSs (Art. 6(13) DMA).

[114]Recital 70 DMA.

In other words, gatekeepers should not design and use manipulative interfaces to reach discriminatory treatment of traders and end users. It follows that neutrality is required of gatekeepers on a permanent basis, as per the type of treatment they reserve to their services and products vis-à-vis those of their competitors. That means that gatekeepers can be liable for circumventing several obligations of the DMA through Dark Patterns. One good example is self-preferencing, prohibited per se under Art. 6(5) DMA. The latter requires the gatekeeper not to treat more favourably, in ranking and related indexing and crawling, its own services and products comparable ones from third parties. Because gatekeepers are bound to apply 'transparent, fair and non-discriminatory conditions to such ranking' to avoid self-preferencing (Art. 6(5) DMA), it should also be illegal to use "Visual Prominence" patterns to self-prefer.

The requirements of transparency, fairness and non-discrimination, read in conjunction with the anti-circumvention rules of Art. 13(6) DMA produce several effects. They may, for instance, impede Amazon from embedding its Amazon Music service into its Alexa voice assistant product by default, unless it also shows rivals' services (such as Spotify, Apple Music, YouTube Music, Tidal, etc.). In addition, they might also allow the Commission to force the gatekeeper to change Alexa's interface design, anytime it demotes competing services by means of a "Visual Prominence" pattern.

4.2.2 | The proposed US AICO Act

The proposed AICO Act is a highly debated bi-partisan antitrust bill that is meant to promote competition and innovation in digital marketplaces where covered firms (largely comparable to the DMA's gatekeepers) operate.[115] Platforms are designated as including firms if they have[116]: (i) at least 50 million active users or 100,000 business users; (ii) an annual market capitalisation or US net sales exceeding US$550 billion, and (iii) serve as a critical trading partner for their business users (meaning that they can act as gatekeeper).[117] Much like the DMA only very large big tech companies would qualify as covered platforms.[118]

Two provisions in the AICO Act mirror those in the DMA which might apply to Dark Patterns alike. Recalling Art. 6(3) DMA, the AICO Act forbids applicable platforms 'to restrict or impede [their] users from … changing default settings that direct or steer covered platform's users to products or services offered by the covered platform operator'.[119] This provision would outlaw "Bad Default" patterns outright. Moreover, applicable platforms cannot 'condition access to the covered platform or preferred status or placement on the covered platform on the purchase or use of other products or services offered by the covered platform operator'.[120] Similar to Art. 5(8) DMA, this provision would outlaw "Forced Subscription" patterns.

4.3 | Assessment: Is user protection widened?

Legislators in both the EU and the US attempt to incorporate collective welfare concerns in Dark Patterns regulation.

[115]For comments, see H. Hovenkamp, 'Gatekeeper Competition Policy', (2023) *Working Paper*, available at https://ssrn.com/abstract=4347768; Yale Tobin Center for Economic Policy, 'International Coherence in Digital Platform Regulation: An Economic Perspective on the US and EU Proposals', (2021) *Policy Discussion Paper No. 5*; D. Geradin and D. Katsifis, 'Selecting the Right Regulatory Design for Pro-competitive Digital Regulation: An Analysis of the EU, UK, and US Approaches', (2021) *Working Paper*, retrievable at https://ssrn.com/abstract=4025419.

[116]Sect. 2(g)(4) AICOA.

[117]Sect. 2(g)(5) AICOA: to be "critical trading partners" covered platforms should have 'the ability to restrict or impede the access of *(A)* a business user to its users or customers; or *(B) a business user to a tool or service that it needs to effectively serve its users or customers*'.

[118]Such as Apple, Google, Amazon, Meta and probably Microsoft. The qualification lasts for ten years (Sect. 2(d) AICOA) but can be removed upon request of the platform demonstrating that it does no longer meets the required criteria Sect. 2(e) AICOA.

[119]Sect. 2(b)(5) AICO Act.

[120]Sect. 2(b)2 AICO Act.

Concerning trust in markets and behavioural market failures, both the DETOUR Act and Art. 25 DSA provide a valuable tool to curb Dark Patterns, especially those practices of big players: the companies concerned can be clearly identified, and the mixture of general clause and possibilities for the enforcers to specify the provisions through guidance provide a certain element of flexibility that allows for the adaption to the dynamic nature of the regulatory object.

Compared to individual-level policies, they both extend the degree of protection, as neither of the two requires the intent of the operator for the practice to be considered a Dark Pattern. Rather, an influence on the autonomous and informed choice or decision in effect is sufficient: they focus on the concrete context, but not the concrete user.[121] What matters is the abstract ability of a concrete design to influence users to behave in a certain way, and empirical findings may also be consulted in this context. This aligns well with the concept of collective welfare protection, because the liberation from the contextual dependency that is attached to the needs of individual market participants allows for the consideration of behavioural market failures and trust in markets to be taken into account when taking actions against Dark Patterns.

However, the scope of the DETOUR Act's provisions is narrower than its European equivalents, because they require practices to be employed '*to obtain consent or user data*'.[122] Hence, those practices that prevent users from discontinuing services would not be illegal under the DETOUR Act. This explicit limitation also prevents the application of the bill to non-transactional use-cases.

Having said that, the DETOUR Act comes with two substantive advantages over the DSA and individual-level policies. First, it prohibits Dark Patterns that may cause, increase or encourage compulsive usage in children,[123] whereas it is questionable whether addiction-inducing design conduct would be included in Art. 25(1) DSA. Second, the DETOUR Act addresses one of the root causes of the problem as to why Dark Patterns are so effective: large-scale A/B-testing[124] that enables a high level of detail regarding knowledge about the behavioural impact of design. The DETOUR Act makes the division of users into groups of study participants—a necessary procedure for A/B testing—dependent on the consent of the respective users.[125] Furthermore, large online operators must disclose the general purpose of such experiments to the users and disclose to the public any experiments with the purpose of 'promoting engagement or product conversion'.[126]

With regard to fair competition and combating data-opolies, both the DMA and AICO Act correctly target only Dark Patterns implemented by gatekeepers, showing that the well-functioning of digital markets is the core priority, not the individual-level one. Their provisions clearly typify illegal Dark Patterns. However, the AICO Act only addresses two transactional Dark Patterns ("Bad Default" and "Forced Subscription"), but leaves Dark Patterns aimed at maximising the collection and sharing of data (akin to Art. 5(2) DMA) uncovered. The reason is probably to be found in the circumstance that data accumulation is not so much perceived as an anticompetitive harm in the US.[127]

The AICO Act does not contain anti-circumvention open-ended provisions, akin to Art. 13 DMA—that could provide flexibility in extending liability of covered platforms for using Dark Patterns to reach anticompetitive goals. Such a provision is relevant, as it overcomes the need to demonstrate much of the context in which transactions occur or consent to data treatment is given, thus including collective welfare harm considerations of promoting fair competition while preventing data accumulation. Furthermore, the DMA takes precedence over data protection and consumer protection laws, being *lex specialis*, thus widening the protection of users against Dark Patterns compared to individual-level policies.

[121]Where enforcers must decide in each individual case whether an online interface sufficiently interferes with the user behaviour.
[122]Sect. 3(a)(1) DETOUR Act.
[123]Sect. 3(a)(3) DETOUR Act.
[124]See note 62. With these practices, large online platforms can conduct externally valid behavioural experiments on a daily basis, giving them a considerable information advantage.
[125]Sect. 3(a)(2) DETOUR Act.
[126]Sect. 3(b) DETOUR Act.
[127]Although the FTC acknowledges the risks of data cumulation by dominant firms (above, n. 89), the DETOUR Act does not implement such concerns. In the EU, on the contrary, Recital 36 and Art. 5(2) DMA consistently pursue data cumulation by Dark Patterns.

Under the DMA, the EU Commission is relieved from the onus of proving that the ex-ante prohibition of using Dark Patterns was violated[128]; however, gatekeepers are not allowed to advocate for any objective justification or an efficiency defence, a possibility that exists in the AICO Act. The latter permits affirmative defences against an action (Sect. 3(b)), meaning that covered platforms can prove—with sufficient levels of evidence—that their conduct would not result in harm to competition or increase consumer welfare and there was no less discriminatory means at its disposal.

Private enforcement is not permitted neither under the AICO or the DETOUR Acts, and the FTC can only demand equitable monetary remedies for consumers in court within the DETOUR Act framework. In the EU, private enforcement is clearly envisaged by the DSA, while it is unclear to what extent it is allowed under the DMA.[129]

From an institutional perspective, the bills proposed in the US are built on the existing enforcement structures and responsibilities, thus sharing enforcement powers among the FTC, the Department of Justice and Attorneys General of individual states (for the AICO Act) or under the FTC solely (for the DETOUR Act). EU legislators, on the contrary, are partially establishing new enforcement regimes that successfully implement collective welfare considerations. Under the DMA, enforcement is facilitated centrally through the European Commission, which enjoys the same investigative and sanctioning powers it has in antitrust cases (including collective redress).[130] The same applies to the DSA, but only where the Commission pursues Dark Patterns used by VLOPs[131] (otherwise the responsibility is borne by national Digital Service Coordinators,[132] resulting in substantial hurdles).[133] The centralisation of competence vis-à-vis VLOPs' conduct is remarkable, since Dark Patterns may involve lots of practices related to how VLOPs process users' data and consent.

5 | LIMITATIONS OF COLLECTIVE WELFARE-LEVEL POLICIES

As Table 4 shows, limitations exist on both sides of the Atlantic that allow the novel legislative measures to achieve the pursued collective welfare goals only to different degrees.

As per policies aimed at tackling behavioural market failures and trust, the greatest constraint consists in the unclear scope of application of Art. 25 DSA. Art. 25 (2) DSA reduces the prohibition of Dark Patterns to instances that do not constitute "*practices covered*" by the GDPR or the UCPD. There are two ways of interpretating this provision, both implying considerable disadvantages for the protection against deceptive or manipulative designs. If this means that Art. 25(1) DSA would not apply to any practice which falls under the scope of applications of the GDPR or the UCPD, it would be an immense limitation, since both scopes of application are notoriously broad. The alternative interpretation is less restrictive but would still adversely affect the efficiency of the provision's enforcement. Understanding "*practices covered*" as practices that are prohibited by the GDPR or the UCPD would require establishing that a specific practice is not illegal under either Regulation before Art. 25(1) DSA could be applied. Consequently, the GDPR and the UCPD would take precedence, meaning that national data protection authorities and entities competent to enforce the UCPD[134] would have to decide that a practice is not prohibited before Art. 25 (1) DSA could be invoked.

This may lead to considerable enforcement difficulties in cases at the national level already, given that the authority to enforce the DSA and to enforce the GDPR or UCPD do not intersect within the same body.[135] The issue

[128]The gatekeepers will instead have to ensure that they comply with all obligations in the DMA.

[129]Art. 39 DMA.

[130]Art. 42 DMA refers to Directive 2020/1828 on representative actions in the field of consumer law, which aims at the facilitation of collectivising consumer interests. This may potentially enable users harmed by DMA violations to seek damages in national courts.

[131]Arts. 51(3) and 82(1) DSA.

[132]Which are to be appointed at the national level, Art. 49 DSA.

[133]It remains entirely uncertain which consequences this entails in Member States. Potentially, a Digital Service Coordinator would have to consult with consumer associations and data protection authorities before acting under Art. 25(1) DSA in such cases.

[134]Depending on the implementation of each Member State, this might vary strongly: H.W. Micklitz and P. Rott, 'Verbraucherschutz', in M.A. Dauses and M. Ludwigs (eds.), *Handbuch des EU Wirtschaftsrechts* (C.H. Beck, 2022), 682 ff.

[135]The national Digital Service Coordinators would have to wait for the relevant authority to decide whether a practice case is prohibited under priority provisions of the GDPR or UCPD (Art. 49 (1) DSA), but that would make enforcement less efficient.

TABLE 4 Assessment of Dark Patterns regulation under collective welfare.

Type of harm	Regulation	Degree of Protection	Weak Points
Behavioural Market Failure Lost Trust in Markets	*DETOUR Act*	Widened: Open-ended provisions No intent required (focus on effect not individual context) FTC may specify provisions Tackles A/B testing Tackles compulsive use of children	Substantive provisions only to obtain consent or data (excludes a number of patterns) No private enforcement
	DSA (only for VLOPs)	Widened: Open-ended provisions + examples No intent required (focus on effect not individual context) EC may specify provisions Enforcement centralised in Commission's hands Collective redress actions permitted	Unclear scope of application of Art. 25(2) DSA (*Individual-level policies repel application of Art. 25 DSA to transactional and data-related Dark Patterns*)
Unfair Competition/ Reinforcement of Data-opolies	*AICO*	Widened: Addresses only covered platforms Allows for firm defence	Only two transactional Dark Patterns covered No provisions for data accumulation No open-ended provisions that extend liability Shared enforcement No private enforcement
	DMA	Widened: Addresses only gatekeepers Open-ended anti-circumvention provisions to curb untypified Dark Patterns Takes precedence over individual-level provisions Enforcement centralised in Commission's hands Private enforcement allowed	Firm defence not permitted

is potentially amplified in cases involving VLOPs, where the EU Commission may take enforcement of Art. 25(1) DSA itself. If in principle centralisation is good, the unclear wording of Art. 25(2) DSA may still frustrate its application.

Effective enforcement options for the Commission therefore remain in two cases. The first of these is when the UCPD or GDPR are evidently not applicable—i.e., in cases of non-transactional user decisions.[136] This happens when Dark Patterns are used as tools for digital influence and the spread of fake news and hate speech. These are considerations that escape the transaction-oriented protection of individuals and instead aim to achieve a prosperous coexistence within our society—also in terms of collective welfare. However, even under this interpretation, the scope of application of Art. 25(1) DSA remains extremely limited for the Commission.

The second case where the Commission has room for intervening against transactional Dark Patterns is when the DSA and DMA overlap, and this happens when VLOPs are also gatekeepers[137] and the conduct is made illegal

[136]Ultimately, however, this is consistent with the results of the first interpretation, which reads Art. 25(2) DSA as covering only cases in which the scope of application of the UCPD or GDPR is not established.

[137]See B. Genç-Gelgeç, 'Regulating Digital Platforms: Would the DSA and the DMA Work Coherently?', (2022) 1 *Journal of Law, Market & Innovation*, 89; K. Bania, 'Designating Large Platforms under the DMA and the DSA: Comparing Apples and Oranges?', (2022) *Blogpost*, retrievable at https://theplatformlaw.blog/2022/09/05/designating-large-platforms-under-the-dma-and-the-dsa-comparing-apples-and-oranges/. Essentially, a provider of CPS that has more than 45 million monthly active users qualifies both as a gatekeeper and a VLOP under the DMA and DSA, respectively.

under both regimes.[138] In such a case, the Commission would gain back its powers to investigate Dark Patterns throughout Europe; however, it could do so only under the DMA framework, not the DSA. In other words, the failure of the DSA to apply to transactional Dark Patterns would be remedied by the DMA, but subject to the conditions established thereby.

As per the AICO Act, the main problems consist in its limited scope of application, restricted to those kinds of Dark Patterns that are aimed at obtaining consent or data (thus excluding a number of practices) and the absence of private enforcement. Concerning policies aimed at ensuring fair competition and preventing data-opolies, the level of protection is widest with the DMA when compared to the AICO Act. Unlike the DMA, the AICO Act focuses only on P2B relationships without including any relevant concerns for end users. In that, it falls short of helping to curb Dark Patterns in a comprehensive way. For instance, it does not contain provisions requiring covered platforms to make end users' service termination possible "without undue difficulty"; nor does it forbid platforms from reiterating consent requests for data treatment if it was refused, and so forth. Dark Patterns affecting end users will remain subject to Section 5 FTC Act's consumer protection provisions.[139]

While it is uncertain if the AICO act will ever become law, it is noteworthy that all violations of the Act also constitute an 'unfair method of competition' under Section 5 of the FTC Act.[140] As said, the FTC intends to revamp the enforcement of such standard according to a highly contested policy statement,[141] hence one might expect that some action will be undertaken by the FTC in its impetus to monitor fairness in digital markets and protect competitors (in addition to competition). In fact, the Commission has repeatedly announced its intention to boost enforcement against illegal Dark Patterns both in its policy statement and staff report of 2021 and 2022, respectively.[142]

The enforcement scenario could be different depending on whether the AICO Act will be adopted or not, as the very conduct (and related standards of proof) might or might not be defined. For instance, lacking the AICO Act, the FTC would need to pursue a "Bad Default" pattern as a standalone Section 5 unfair methods of competition situation. However, while Section 2(b)(5) AICO Act provides a definition of the forbidden practice ("restrict or impede users from [...] changing default settings that direct or steer [them] to products or services offered by the [same] covered platform"), nothing similar exists with unfair methods of competition cases. Here, the FTC would need "creativity" to build a standalone case that departs from established antitrust caselaw. Hence, to pursue a "Bad Default" pattern it should pick one of the conducts out of the list contained in its Section 5 enforcement statement, and then engage in the overly burdensome exercise of building on it. Among the many, the one that seems more suitable in terms of effects on the market is "de facto tying [or] bundling ... that use market power in one market to entrench that power or impede competition in the same or a related market".[143]

Concerning the DMA, some level of legal uncertainty remains per those Dark Patterns that are prohibited if used for circumvention purposes in the DMA and those that require specification by the Commission under Art. 6 DMA. For instance, given the vagueness of expressions such as "easily change" or "steering users" one would expect that without further clarification, Art. 6(3) DMA will not be applicable in a near future to contrast Dark Patterns.

[138]See Table 1 above.
[139]See Section 4.1 above.
[140]Sect. 2(h)2 AICO Act.
[141]Federal Trade Commission, 'Policy Statement Regarding the Scope of Unfair Methods of Competition Under Section 5 of the Federal Trade Commission Act Commission', (2022b) *File No. P221202, November 10, 2022*. For a critical assessment, see US Chamber of Commerce, 'The FTC's New Section 5 Guidance', (2021) *Blogpost*, retrievable at https://www.uschamber.com/finance/antitrust/the-ftcs-new-section-5-guidance-what-you-need-to-know; S. Salop and J. Sturiale, 'The FTC Should Quickly Issue New Section 5 Enforcement Guidelines', (2022) *Blogpost*, retrievable at https://www.promarket.org/2022/07/26/the-ftc-should-quickly-issue-new-section-5-enforcement-guidelines/.
[142]See FTC (2021) and (2022a) above, n. 44.
[143]FTC (2022b), above, n. 141, at 14.

6 | NORMATIVE IMPLICATIONS OF THE COLLECTIVE WELFARE APPROACH TO DARK PATTERN REGULATION

Even beyond the highlighted limitations of incoming and novel legislation, the collective welfare approach presented in this article offers potential advice for policymakers as well as public authorities tasked with enforcement. This allows us to make proposals on concrete criteria for guiding the enforcement of relevant provisions (Section 6.1) and to suggest amendments to new and proposed legislation (Section 6.2).

6.1 | Guidance for enforcing authorities: a risk-based approach

The preceding analysis has revealed those elements of the European and the US legal systems that already provide varying degrees of protection against the use of Dark Patterns. Both legal systems now strive to create additional protection against these practices through extensive general clauses as well as regulations that depend on the size of the company to be regulated and the impact of their practice. Further guidance from the enforcing authorities is needed to specify these general clauses and thus create an appropriate level of legal certainty for both designers and users of digital interfaces. In Europe, this task is explicitly stated in Art. 25(3) DSA[144] and under Art. 6 DMA (which requires specification acts). In the US, the FTC has issued guidance only on "Forced Subscription" patterns, while more extensive guidance on which practices are prohibited is expected in general and would be recommended in B2B practices.

Entrusting enforcers with the power to issue guidelines on specific design practices seems appropriate, since it is more feasible for the administrative level to consider these transmission channels while issuing such guidelines, than for every enforcing authority to become aware of behavioural science and the concrete effects of manipulation. It thus appears to be an efficient solution to transfer this process to the EU Commission or the FTC, which can consider behavioural insights when issuing the respective guidance. At the same time, this provides a certain amount of flexibility for the enforcers, which may update their guidance on a rolling basis to account for changes in the dynamic Dark Pattern landscape.

By using a risk-based catalogue of decision criteria,[145] agencies can address those practices that have most impact on collective welfare dimensions. Explicitly, focusing on the interaction of the "influence" of specific practices, the economic significance of the "context" in which they are employed, as well as the "scope" of users reached by specific corporations can inhibit the exploitation of behavioural market failures, strengthen confidence in markets and protect fair competition.

6.1.1 | Influence

Manipulative design practices that fall under the term "Dark Patterns" can differ strongly on a case-by-case basis. This also applies to the influence they potentially exert on the behaviour of users. The influence that each pattern may have on the respective decision of users depends strongly on the individual case, its specific configuration and the context it is employed in. Only a handful of experimental studies compare the effects of different Dark Patterns

[144]The Commission is not subject to any constraints in the formulation of its guidance. However, for Dark Patterns explicitly mentioned in Art. 25 (3) DSA ("Visual Prominence", "Nagging", "Roach Motel", "Click Fatigue" and "Bad Default"), guidance should "notably" be issued. Recital 67 DSA mentions additional practices for which guidance "may" be expected. These are: "Click Fatigue" and "Bad Default" patterns.

[145]See also Q. Weinzierl, 'Dark Patterns als Herausforderung für das Recht', (2020) 39 *Neue Zeitschrift für Verwaltungsrecht Special Issue 15*, 1, 7.

in similar situations, for example within the context of cookie banners[146] or in the broader context of consumer transactions.[147]

There is too little empirical evidence to extrapolate a somewhat precise account for this parameter in practice. To do so, authorities would need a more accurate idea of which designs affect the behaviour of the user and to what extent. Gathering this insight through experimental research is very costly and time-consuming. In an environment as dynamic as the market for design of online interfaces, it seems questionable whether the influence of certain designs can be researched conclusively or even fairly contemporaneously, or whether instead users adapt to certain design patterns, which in turn leads websites to adjust their designs as well.[148] Without these data, only a broad estimation of the intensity of different Dark Patterns can be used for determining their influence.

However, an extensive amount of information on the question of which designs influence user behaviour in which way *does exist*—but is not publicly available. By using A/B testing, website operators essentially run large-scale field experiments every day. This allows them to pinpoint the exact influence of their design choices on user behaviour. There is hardly any public information on the magnitude with which this really takes place; evidence of such practices remains anecdotal at best.[149] However, given the fact that large internet platforms operate in a highly data-driven manner, it seems reasonable to assume that they hold immense insights into the impact of design on human behaviour. If the enforcing authorities gained access to this information, the assessment of the influence of Dark Patterns could be much more precise and be utilised for the risk-based assessment.

6.1.2 | Context

The second element in the risk-based assessment is the potential economic and normative harm that design patterns may impose on users. To evaluate the gravity of the consequences, it is important to consider the context in which Dark Patterns are employed. In the context of e-commerce transactions, this aspect can be quantified easily via the associated price: if Dark Patterns encourage a user to take up a monthly magazine subscription for $5, this has a different economic significance and lower potential harm than if the user is persuaded to take out a $2000 consumer loan before going on a vacation. With this in mind, it seems reasonable to define certain contexts in which protection against the influence of Dark Patterns will generally be of particular importance. Establishing a context-dependent protective concept that differs between choice environments that typically have a higher or lower economic consequence for the user thus seems advisable.

This approach is straightforward in contexts where there is a quantifiable and measurable economic harm. It is less so in situations where the harm is not easily quantified. Where deceptive designs influence, for example, privacy decisions, there will be variations in the gravity of the choice: disclosing one's email address will have less significance than sharing financial contract information or political opinion. The users' valuations and market relevance of these different data, however, vary in normative assessment. This makes it difficult to

[146]C. Utz et al., '(Un)informed Consent: Studying GDPR Consent Notices in the Field', (2019) *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, retrievable at https://doi.org/10.1145/3319535.3354212, 9 identifies an influence of 11.6 percentage points for users with mobile phones in a large-scale field experiment. D. Machuletz and R. Böhme, 'Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR', (2020) *Proceedings on Privacy Enhancing Technologoies*, 481, 491 identify a 20.9 percentage point increase for desktop users in a quasi-lab experiment in class with students.

[147]Luguri and Strahilevitz, above, n. 3, 58–82 reveal a differing influence of the designs on behaviour: "Hidden Information", "Trick Question" and "Click Fatigue" patterns were found most successful in manipulating behaviour and more aggressive patterns generally seemed to be more influential—up to a certain point: very aggressive designs led subjects to quit the experiment altogether. The authors thus conclude that the most dangerous patterns are those which are relatively subtle. See also A. Zac et al., 'Dark Patterns and Online Consumer Vulnerability', (2023), *Working Paper*, retrievable at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4547964, which focuses on different concepts of consumer vulnerability.

[148]There is evidence that "Scarcity" patterns ('*only 2 hotel rooms left!*') have become less effective over the last few years; see S. Shaw. 'Consumers Are Becoming Wise to Your Nudge', (2019) *Blogpost*, retrievable at https://behavioralscientist.org/consumers-are-becoming-wise-to-your-nudge/.

[149]Google once tested more than 40 different shades of blue on their impact on the clickthrough rate, above, n. 31.

establish universally valid guidelines for the amount or type of data that deserve special protection (the European GDPR only refers to personal data, while Dark Patterns, in a market-wide context may also include non-personal data).

In some cases, enforcers might overlook the latter metrics and prefer to consider the target audience of an offer. This may be the case for Dark Patterns whose content is aimed at children or senior citizens—two groups which may on average be more susceptible to manipulative designs.[150] The need to enhance collective welfare may justify special safeguards against undue influence for those groups. Empirical findings also suggest that people with a lower level of education (measured in terms of formal qualifications) are more likely to be influenced by Dark Patterns.[151] All of this should be considered when factoring in context, because different audiences may be influenced with different levels of ease.

6.1.3 | Scope

The last aspect of our risk-based evaluation approach is probably the most evident: the range of Dark Pattern usage. This considers how many users are interacting with the digital system that employs Dark Patterns and therefore are potentially exposed to their influence. This aspect can be particularly helpful for authorities in prioritising who to target first. Within this component, the collective welfare approach becomes all the more evident. Considering the scope of influence of a specific practice shifts the focus from individual-based protection to market-based protection. This is done by regulating the most wide-ranging actors more intensively, especially those who regularly serve as role models in the market. If they use better design standards (due to more effective enforcement), this also strengthens trust in markets.

Another direct economic criterion is the *number of transactions* or number of simple direct contacts (like scrolling or scraping): if a company conducts more transactions or has more direct contacts with users, the employment of Dark Patterns is likely to lead to a higher number of users being influenced, and this increases the absolute amount of damage caused.

Such considerations have been implemented by each of the legislative acts discussed here: the DSA sets up a more efficient centralised enforcement regime for VLOPs, the DMA exclusively focuses on gatekeepers, the AICO Act aims to cover platforms with 50 million active monthly users, and the DETOUR Act aims to cover online operators with more than 100 million authenticated users in a 30-day period. Already under existing laws, this focus on market relevance can be implemented by concentrating enforcement activities on companies that carry out a particularly high volume of transactions or by considering the number of direct contacts (like the DSA) in the market. Such enforcement focus would also effectively protect the collective welfare considerations presented in this article.

6.2 | What legislators could do

The main recommendation to legislators concerns the clarification of the scope of Art. 25(1) DSA. The added value of substantive protection that the DSA can provide in its current form is modest at best. Even if this provision opens the prohibition of Dark Patterns to new non-transactional contexts, and although it opens the doors to considerations of collective welfare, its main benefit is largely a symbolic one. In order to ensure effective enforcement, the restriction of Art. 25 (2) DSA would have to be clarified and, ideally, the clause giving precedence to data and consumer protection laws removed.

[150] Bongard-Blanchy et al., above, n. 53.
[151] Luguri and Strahilevitz, above, n. 3, 70 f.

With regard to the AICO Act and the DMA, the collective welfare approach is more visible, as these specifically target the most influential market participants to improve market practices for the benefit of users. At the same time, it would be advisable that these legislative measures establish the targeted authors of Dark Patterns in a more harmonised way, given that the criteria for establishing who the addressees are differ sensibly. This might jeopardise the level of legal protection provided to users in both the EU and the US or, at best, could generate a potential "Brussels Effect".[152]

Moreover, to gather information on the influence of Dark Patterns over the market,[153] the approach of the DETOUR Act to prohibit A/B testing without users' consent could be adopted also in the EU and be more usefully be complemented by a right of enforcing authorities to access to the information about how user behaviour is altered through design decisions, i.e., the results of companies' A/B testing. In the end, the issue of A/B testing and asymmetries around it is a recurring central problem: whether it is the ability of enforcers to get access to such data, or consumers' ability to opt out from "Bad Default" patterns, or the firms' ability to stay ahead of consumers' ability to adapt, A/B testing plays a pivotal role.

7 | CONCLUSION

Dark Patterns are a phenomenon that has already attracted the attention of legislators in both the EU and the US. Both jurisdictions have existing regimes in place to address these practices. The DSA and DMA in the EU, as well as the proposed DETOUR and AICO Acts in the US, are aimed at further curbing these practices. This occasion marks a change in regulatory perspective, with frameworks no longer aiming solely at protecting individual consumers, but taking market-wide considerations into account by increasingly addressing collective welfare considerations.

In part, these efforts have been somewhat unsuccessful: the DSA in particular—despite good intentions—only marginally improves the de facto level of protection. The DMA, on the other hand, provides substantial added protection for collective welfare by streamlining enforcement systems and targeting the key players in the market. The DETOUR Act and AICO Act, if passed, would also noticeably expand the scope of protection in favour of users.

Even though these novel regulations are only partially successful in their endeavour to increase the protection against a widespread use of Dark Patterns, the shift towards a collective welfare perspective can still pose a viable tool to advance efficient enforcement. The risk-based enforcement strategy proposed in this article considers the behavioural influence of the design patterns, the material context in which it is employed, and the scope of the audience reached by the practice in question. Enforcing authorities that are interested in maximising the impact of their enforcement agenda can consider these criteria when deciding which cases to concentrate on or prioritise in prosecuting or providing further guidance.

These enforcement considerations can be considered by both EU and US authorities. In addition to the material convergence outlined in this article, this may also lead to convergence in terms of enforcement. This would be a welcomed development, as neither the prevalence of Dark Patterns nor the consumption of digital services is bound by geographical borders. A transatlantic harmonisation of legal standards therefore reflects the international nature of the phenomenon. The ability to exchange expertise gained from guidelines and rulings may give policymakers and enforcement authorities from both jurisdictions a chance to keep up with rapidly evolving design practices and knowledge advantage that digital companies currently have about the effect of interface design. Instead of engaging in regulatory competition, both legal systems may thus mutually benefit each other to strengthen the protection of consumers and data subjects in both legal systems. The collective welfare approach can therefore be considered as important for both the EU and the US.

[152]See A. Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2019), explaining the concept behind the alleged "Brussels Effect" in chapter 2.

[153]See above, Section 5.2.1.1.

ACKNOWLEDGEMENTS

We are thankful to Michal Gal, Ramsi Woodcock, Salil Mehra, Fabrizio Esposito and the participants in the 2023 ASCOLA annual conference for providing very useful comments to previous versions of this paper.

ORCID

Fabiana Di Porto https://orcid.org/0000-0002-4420-9741
Alexander Egberts https://orcid.org/0009-0009-8504-3678

How to cite this article: Di Porto F, Egberts A. The collective welfare dimension of dark patterns regulation. *Eur Law J*. 2023;29(1-2):114-141. doi:10.1111/eulj.12478