cerre Centre on Regulation in Europe

HARMFUL ONLINE CHOICE ARCHITECTURE

REPORT

May 2024

Christoph Busch
Amelia Fletcher

cerre

Report

Harmful Online Choice Architecture

Christoph Busch
Amelia Fletcher

May 2024

As provided for in CERRE's bylaws and procedural rules from its “Transparency & Independence Policy”, all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which this report has been prepared, received the support and/or input of the following CERRE member organisations: Arcom, Amazon, DuckDuckGo, Ofcom, Mozilla, and TikTok. The authors are also grateful to ACM for their valuable contributions to the project. The member organisations bear no responsibility for the contents of this report. The views expressed in this CERRE report are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor, or of members of CERRE.

info@cerre.eu – www.cerre.eu

Table of Contents

About CERRE

Providing top quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) promotes robust and consistent regulation in Europe's network and digital industries. CERRE's members are regulatory authorities and operators in those industries as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach;
- the widely acknowledged academic credentials and policy experience of its team and associated staff members;
- its scientific independence and impartiality;
- the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to network industries and the markets for their services.

CERRE's activities include contributions to the development of norms, standards and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological, and social environment. CERRE's work also aims at clarifying the respective roles of market operators, governments, and regulatory authorities, as well as at strengthening the expertise of the latter, since in many Member States, regulators are part of a relatively recent profession.

About the Authors

Amelia Fletcher CBE is a Professor of Competition Policy at the Centre for Competition Policy, University of East Anglia and co-editor of the Journal of Competition Law and Economics. She also acts as an expert witness.

She has been a Non-Executive Director at the UK Competition and Markets Authority (2016-2023), Financial Conduct Authority (2013-20) and Payment Systems Regulator (2014-20), and a member of Ofgem's Enforcement Decision Panel (2014-2022). She has also been a member of DG Comp's Economic Advisory Group on Competition Policy, and was a member of the Digital Competition Expert Panel, commissioned by the UK Treasury and led by Jason Furman, which reported in March 2019.

She was previously Chief Economist at the Office of Fair Trading (2001-2013), where she also spent time leading the OFT's Mergers and Competition Policy teams. Before joining the OFT, she was an economic consultant at Frontier Economics (1999-2001) and London Economics (1993-1999).

She has written and presented widely on competition and consumer policy. In her ongoing research, Amelia has a particular interest in the implications for competition and consumer policy of behavioural economics and online markets.

Amelia has a DPhil and MPhil in economics from Nuffield College, Oxford.

Christoph Busch is Professor of Law and Director of the European Legal Studies Institute at the University of Osnabrück, Germany. He is a Fellow and Council Member of the European Law Institute (ELI) and an Affiliated Fellow at the Information Society Project at Yale University. His research focuses on consumer law, platform governance and algorithmic regulation.

Executive Summary

Any digital interface or system which allows users to make choices will inherently include 'online choice architecture'. This simply refers to the way in which choices are framed in a connected environment. The term itself is neutral: in many cases, the design choices made by 'choice architects' (here, typically 'UX designers') are helpful and convenient for users. However, there is growing evidence of harmful online choice architecture, which worsens users' decisions rather than helping them. As well as directly harming users, this can have knock on effects for the effective functioning of markets, and even society.

The appropriate legal treatment of such harmful online choice architecture is highly topical. It is a key issue in a fast-growing list of competition and consumer protection cases, as well as a multitude of recent reports by authorities, consumer bodies and academics. The European Commission is currently conducting a fitness check of EU consumer law,[1] which could potentially lead to a "Digital Fairness Act" to be presented early in the next Commission's mandate. A key issue to be considered as part of this review is the adequacy of consumer protection laws to address harmful online choice architecture.

In addition, rules relating to online choice architecture are increasingly arising across a variety of other areas of EU legislation and associated guidance, beyond consumer protection law. This includes the General Data Protection Regulation (GDPR), the Digital Markets Act (DMA), the Digital Services Act (DSA), the Data Act (DA), and the AI Act (AIA), as well as addressing harmful online choice architecture by firms.

This growing array of legislation gives rise to risks of fragmentation, overlap, and inconsistency, as well as risks that the laws are either ineffective or have unintended harmful side effects.

Against this background, this report analyses the different conceptual approaches to harmful online choice architecture (Section 1); maps and discusses the rapidly expanding regulatory landscape (Section 2); formulates ten principles for effective policy for addressing harmful online choice architecture (Section 3); and draws out 20 actionable recommendations for policymakers (Section 4).

The ten principles we identify are:

- **Principle 1:** Do not restrict regulation to only addressing 'intentional' harmful effects.
- **Principle 2:** Regulation should be clear about the 'mechanism of effect on users', but not be restricted only to 'deceptive' online choice architecture.
- **Principle 3:** Regulation should be clear about the nature of the harm involved, and who it pertains to.
- **Principle 4:** Recognise intrinsic limits to informed and autonomous decision-making.
- **Principle 5:** Recognise that context is important for assessing online choice architecture – it can be beneficial, as well as harmful, and can be used positively.

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en

- **Principle 6:** Exercise of rights should be easy and not undermined by online choice architecture.
- **Principle 7:** Ensure that regulation addresses online choice architecture across multiple user path elements.
- **Principle 8:** Consider special rules for automated personalised choice architecture.
- **Principle 9:** Behavioural testing should be encouraged, or even required in specific circumstances, and regulators should be able to access test results.
- **Principle 10:** Mitigate risks of regulatory overlap or inconsistency.

Our objective with this report is to contribute to the policy debate on the forthcoming revision of European consumer law, on the basis of the Digital Fairness Fitness Check and the resulting elaboration of a Digital Fairness Act, as well as to further the regulatory design and implementation designed to address harmful online choice architecture.

1. Harmful Online Choice Architecture Definitions: Why Do We Care?

In this section, we start by discussing the nature of 'online choice architecture' and how it can be harmful. We then consider different possible definitions, including summarising the terms used in the existing EU regulatory framework.

1.1 What Is Online Choice Architecture?

'Choice architecture' is a term describing the design of the environment within which choices are made. This can comprise the way in which choices are framed, but also the whole user journey, such as how many steps any choice involves.

Whilst it has long been relevant in an offline environment, **the impact of choice architecture is amplified in an online environment**.[2] And by 'online' choice architecture, we do not only mean website design but also choice architecture within connected digital environments. For example, it would include the choice of a search engine or browser on a digital device, an issue that is addressed under the EU Digital Markets Act (DMA).

The amplified impact of choice architecture in an online environment, relative to offline, partly reflects the importance of the user interface for online choices. Essentially, it is impossible to design a website without incorporating some type of choice architecture, even if this only relates to what to place most prominently on the page. In this sense, there is no such thing as a perfectly 'neutral' design of online user interfaces, albeit some designs can clearly be better than others at enabling users to make choices that broadly align with their preferences. An additional element which is amplified online is the ability of 'choice architects' to test alternative designs, and to collect data about their impact, sometimes on a huge scale.

It is well understood that **choice architecture (both off- and online) can have a substantial effect on the choices that people make**. For instance, there is extensive academic literature, and many practical examples, of people exhibiting:[3]

- 'Default effects' (propensity to choose the 'default' option);
- 'Ranking effects' (propensity to choose more highly ranked options);
- 'Salience effects' (propensity to choose more salient or prominent options);
- '*Status quo* effects' (propensity to stick with the current option); or,

[2] Note that we use the term 'online' but this should not be taken to relate only to website design but connected digital environments more generally. For example, it would include the choice of search engine or browser on a digital device, and issue that is addressed under the EU Digital Markets Act.

[3] It is beyond the scope of this report to provide complete references on the various behavioural effects mentioned, but an excellent review of the evidence is provided in the evidence review section of Competition and Markets Authority (2022) *Online Choice Architecture: how digital design can harm competition and consumers*, https://www.gov.uk/government/publications/online-choice-architecture-how-digital-design-can-harm-competition-and-consumers.

- 'Social influence/popularity effects' (propensity to choose options selected or recommended by others, or more popular options).

Words and colours can also play an important role:

- For example, as we might expect, people are more likely to press buttons that are green and include simple positive wording such as '*Yes please'.* They may also choose things accidentally if the wording is presented confusingly (such as with double negatives), or if key information is in a font colour similar to the background.
- By contrast, warnings may be more effective if shown in bold or red and if they include forceful and complex wording such as "Your phone and personal data are more vulnerable to attack by unknown apps. By installing apps from this source, you agree that you are responsible for any damage to your phone or loss of data that may result from their use."[4]

A key underlying driver of these various effects is that the process of careful deliberative decision-making takes time and effort. Over time, people have both evolved and learned to take shortcuts by using rules of thumb – or "simple heuristics that make us smart" (Gigerenzer et al, 2000)[5] – sometimes known as 'System 1 thinking' (Kahneman, 2011).[6]

These rules of thumb can be helpful, and indeed choice architecture is itself a neutral term, in that the use of defaults, prominence, rankings, etc., can help people make decisions that reflect their underlying preferences. Indeed, the fact that choice architecture can be useful arguably contributes to its power. Evidence on 'default effects' shows that these are strongest when people perceive the default as an implicit 'endorsement' of this choice by someone who has thought carefully about the available options.[7]

However, the effects of choice architecture can also be harmful. This can occur inadvertently: indeed, it is impossible to design perfectly 'neutral' choice architecture. However, harmful choice architecture can also be intentional, designed not in the chooser's interest but rather in the interest of the 'architect', which is typically a firm that stands to gain from poor choices. In the context of online consumer choices, this means the online environment being designed in the interest of the supplier not the consumer.

In addition, the behavioural effects described may be stronger in contexts where people find choices harder. For example, people can face:

- 'Information overload' (propensity to make worse choices when given too much information);
- 'Choice overload' (propensity to make worse choices when offered too many options);
- 'Choice fatigue' (propensity to make worse choices when asked to make too many choices, or the same choice too many times, for instance via repeated 'pop-ups'); or,

[4] Warning used during the sideloading process on Android phones at the time of the CMA 2019 market study into mobile ecosystems.
[5] Gigerenzer, G., Todd, P. M. and ABC Research Group (2000) *Simple Heuristics that Make Us Smart*, Oxford University Press.
[6] Kahneman D. (2011) *Thinking Fast and Slow*, Farrar, Straus and Giroux.
[7] Jachimowicz, J.M. et al. (2019) 'When and why defaults influence decisions: a meta-analysis of default effects', *Behavioural Public Policy*, 3(2), pp. 159–186. doi:10.1017/bpp.2018.43.

- 'Complexity aversion' (propensity to avoid seemingly complex choices in favour of simpler ones).

In some cases, such factors can put people off making any decision at all, thus increasing *status quo* effects. Alternatively, people may make worse choices. This can be worsened when they are put under pressure, for example, if they feel time-constrained. Even apparently small frictions, such as having to make additional clicks, can deter people from acting (an effect that can have both positive and negative implications). **These issues also mean that well-intentioned policy could, in some cases, either be ineffective or have unintended negative effects.** For example, a policy designed to enhance the information or choices available to consumers in fact risks worsening decision-making due to information overload or choice fatigue.[8]

These **behavioural effects are not limited to specific people; they are exhibited by all of us**, although the types and extent of effects can vary across individuals and across contexts.

Finally, we note that there is a close link between online choice architecture and algorithmic recommendations/curation. The power of such recommendations will be affected by the online choice architecture within which they are provided. For example, consumers are more likely to choose a specific recommendation if it is given very strong prominence (for example, in a vertically ranked list of search results) than if recommendations are laid out more neutrally in a horizontal list. However, algorithmic recommendation systems/curation raise additional issues, beyond the associated online choice architecture, and thus they are not a focus in this report.

1.1.1 Beneficial Online Choice Architecture

As already mentioned, 'choice architecture' is a neutral term, and well-designed online choice architecture can have important beneficial effects. For instance:

- Adding small frictions to a decision-making process can be a useful way of ensuring that individuals are aware of any choice they are making, encouraging them to contemplate that choice more carefully.[9]
- Online choice architecture which sets out different options (such as prices or similar products) in a clear and easily comparable way can be valuable in helping consumers to choose amongst those options.

The focus of this report is on harmful online choice architecture. However, as the flipside to this, we note that policy makers can also use choice architecture proactively as a positive enabler of consumer choice. This can be done either generally, such as with requirements that certain actions should be 'easy', or more prescriptively, such as with specific requirements around cancellation buttons.

It should also be noted that online choice architecture can potentially be at once beneficial and harmful, for different recipients. For instance, many consumers will value the convenience offered by

[8] For example, the requirements for cookie consent under the EU's ePrivacy directive is widely considered to have led to such choice fatigue. In response, the Commission has recently developed a draft "cookie pledge", intended to reduce the frequency with which cookie consent is sought. https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/cookie-pledge_en

[9] For example Jahn et al (2023) find that friction interventions, which make the sharing of content more cumbersome, can be useful in curbing the spread of misinformation of social media. https://doi.org/10.48550/arXiv.2307.11498.

the fact that mobile devices typically come 'ready to use', with a variety of apps and services included by default. However, some consumers may then end up with apps that are not those they would have chosen had they been given an option, and rival apps will struggle to win customers, even if they are better or more suitable. Similarly, pop-up windows that provide retention offers to consumers who are about to cancel a subscription may be useful for some consumers, while being annoying for others.

Theoretically, assessing the overall impact of such online choice architecture requires a 'weighing up' of the net effects across parties relative to a counterfactual (which might involve alternative defaults or requirement of active choices). In practice, however, such analysis can be near-impossible to do; for instance, it is far from obvious what weights one should use.

As such, policy design and implementation is more often focused on overcoming the negative effects on one group, unless there are very clear and strong countervailing benefits to others. For example, policy concerns relating to the lack of competition in search engines are so strong that the DMA prioritises the promotion of competition, by introducing a search screen, over the interest of consumers in having a smooth consumer journey. The 'weighing up' of harmful and beneficial effects is especially unlikely to be considered appropriate where the individuals that lose out are vulnerable or disadvantaged.

We would note that there is also a fine line to be drawn between harmful online choice architecture and legitimate marketing practices. Sometimes this may be a matter of degree. For example, pop-up prompts can be useful for encouraging consumers to consider particular products, but excessive pop-up prompts can lead to them accidentally making poor choices. Likewise, we know that people really value a sense of identity and community,[10] and in that context, advertising via social influencers can provide a useful way of framing products to align with how particular groups of people see themselves. But if those social influencers provide their messages without disclosing their intent (that is, not clearly flagging them as advertising), this approach risks veering from merely persuasive into misleading.[11]

1.1.2 Harmful Online Choice Architecture

Turning now to harmful online choice architecture, we note that there has been a panoply of words used to describe this phenomenon. Perhaps the most widely used to date has been 'dark patterns', a term coined and popularised by User Experience (UX) Designer Harry Brignull in 2010. However, Brignull's website has itself recently revised this term to 'deceptive patterns' (and consequently renamed itself), to avoid any risk of inadvertent negative associations with harmful stereotypes.[12]

[10] See generally Akerlof and Kranton, *Identity Economics,* Princeton University Press, 2010.

[11] Luguri and Strahilevitz (2021) propose that 'dark patterns' (i.e., harmful choice architecture) be distinguished by its impact in manipulating recipients into a choice inconsistent with their preferences, whereas marketing efforts seek to alter those preferences. But in fact, as will be discussed below, online choice architecture can also alter preferences.

[12] See footer of his current website: https://www.deceptive.design/about-us. See also Brignull, H. (2023) Deceptive patterns – exposing the tricks that tech companies use to control you. In our view, the term 'deceptive patterns' does not seem be an entirely accurate description for all types of harmful design patterns. For example, the categories 'nagging' and 'obstruction' do not necessarily involve a deceptive behaviour, but are rather aggressive commercial practices.

Brignull's website defines 'deceptive patterns' as **"tricks used in websites and apps that make you do things that you didn't mean to".** His site and associated book describe an array of types of harmful patterns, which primarily relate to supplier-consumer relationships:

- 'Comparison prevention' (Bundling or framing products in different ways so that they are harder to compare)
- 'Confirmshaming' (Using words that are designed to trigger shame)
- 'Disguised ads' (Blurring the line between content and advertising, so that ads might appear to be content)
- 'Fake scarcity' (Untrue or misleading low stock or high demand messages)
- 'Fake social proof' (Falsified or exaggerated endorsements, reviews, or ratings)
- 'Fake urgency' (Unnecessary use of time pressure)
- 'Forced action' (Requiring consumers wanting to do one thing to do something else too)
- 'Hard to cancel' (Also known as 'roach motel') (Making it easy to subscribe or sign up but hard to cancel)
- 'Hidden subscription' (Enrolling in a user in a recurring subscription or payment plan without clear disclosure or explicit consent)
- 'Nagging' (Persistent requests to do something)
- 'Obstruction' (Hurdles placed in the way of completing a task or accessing information)
- 'Preselection' (Presenting a default option)
- 'Sneaking' (Withholding or obscuring relevant information, such as additional costs or unwanted consequences)
- 'Trick wording' (Using confusing or misleading language)
- 'Visual interference' (Hidden, obscured or disguised information, for example by using small, low contrast text).

Although this is a long list, others have suggested additional examples. Indeed, Singh et al (2023) provide a list of 50 'dark patterns' prevalent in e-commerce.[13] Terminology can also differ, for instance 'sneaking' is often referred to as 'drip pricing'.

While Brignull uses the term 'deceptive patterns' on his website, he has more recently adopted the alternative term 'harmful design', recognising that design need not be deceptive in order to be harmful.[14] Others are also using this term, or the slightly extended 'harmful design patterns', while

[13] Singh, V. et al (2023) 'Prioritizing dark patterns in the e-commerce industry – an empirical investigation using analytic hierarchy process', *Measuring Business Excellence.*
[14] See https://research.mozilla.org/files/2024/01/Over-the-Edge-Report-January-2024.pdf

Richard Thaler, who co-wrote the 2008 book 'Nudge', has coined a new term 'sludge' to refer to the deliberate use of friction to deter consumers from acting in their own interest.[15]

In this report, we use the term 'harmful online choice architecture', partly because we feel some of the other terms risk being too narrowly defined. We note that this is also the preferred term used by the UK Competition and Markets Authority in their work in this area.[16]

1.2 Defining Harmful Online Choice Architecture

Drawing on the list of 'deceptive patterns' outlined in Section 1.1.2, it is possible to describe a number of key aspects of harmful online choice architecture, or at least what it is not.

First, harmful online choice architecture need not be false. Firms can steer consumers in an unsuitable direction, for instance by presenting an option as a default or in confusing or alarmist language, without saying anything that is strictly untrue. Some online statements about available stock have been found to be entirely false, for example, with the stock level shown to decrement according to a recurring, deterministic schedule.[17] But even true available stock statements have the potential to be misleading if framed in an alarmist way.

Second, context matters. In some contexts, consumers may find it useful to know how much stock there is left of a product or how much time is left to order an item so that it arrives before Christmas. Likewise, if a consumer has already actively chosen to go down a particular sales route, a pre-selected option (such as 'go to checkout') may be useful in enabling a smoother consumer journey. However, in other contexts such choice architecture can create undue pressure or steer people towards unwanted options.

Third, harmful online choice architecture need not be intentional or deceptive. Brignull's discussion of deceptive patterns refers to them as 'deliberately deceptive'. This would seem to imply both **intent** on the part of the designer and an outcome in which consumers are **deceived** – that is, believe something that is untrue. However, many have argued – and we agree – that this definition is too restrictive. Online choice architecture can be harmful even where this is unintentional and even where there is no deception. For example, some harmful design patterns such as 'nagging' or 'obstruction' do not necessarily involve any deceptive behaviour, but are rather better viewed as 'aggressive' commercial practices.

However, none of this helps us towards a positive definition of harmful online choice architecture. In fact, it turns out that agreeing to a precise definition is far from straightforward. While there have

[15] Richard H. Thaler. 2018. 'Nudge, not sludge'. Science 361, 6401 (2018), 431–431. https://science.sciencemag.org/content/361/6401/431.full.pdf

[16] Competition and Markets Authority (2022) Online Choice Architecture: how digital design can harm competition and consumers, https://www.gov.uk/government/publications/online-choice-architecture-how-digital-design-can-harm-competition-and-consumers.

[17] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., and Narayanan, A. (2019). "Dark Patterns at Scale: Findings from a Crawl of 11k Shopping Websites." Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1–32. https://doi.org/10.1145/3359183

been a variety of attempts at definitions (albeit usually of 'dark patterns'), there is no universally accepted definition.

We consider that the following definition from the OECD (2022) does have some merit, although it remains fairly broad and relates to 'dark commercial patterns':

> *"Dark commercial patterns are business practices employing elements of digital choice architecture, in particular in online user interfaces, that subvert or impair consumer autonomy, decision-making or choice. They often deceive, coerce or manipulate consumers and are likely to cause direct or indirect consumer detriment in various ways, though it may be difficult or impossible to measure such detriment in many instances."*[18]

As discussed further below, we believe it would be useful to employ more aligned and consistent definitions across legislation. However, we would not propose a single definition that applies horizontally across different legal instruments, not least because the relevant context for each application within legislation will be different.

However, drawing on work by Mathur, Mayer, and Kshirsagar (MMK, 2021),[19] we would encourage anyone engaged in such a definition to consider four elements that may be relevant (although none is straightforward).

1. **The nature of the online choice architecture**: 'Deceptive patterns' are often considered to relate to 'online user interfaces', but harm can also arise from how these interfaces fit together as 'user journey'. This is all part of the overall choice architecture.

2. **The mechanism of effect on users**: MMK identify thirteen such mechanisms. Harmful online choice architecture can: attack users; confuse users; deceive users; exploit users; manipulate users; mislead users; steer users; subvert user intent; subvert user preferences; trick users; undermine user autonomy; make choices without user consent; or make choices without user knowledge. However, we note that the distinctions between some of these concepts is blurry, and that some of these mechanisms (such as steering consumers) can be beneficial depending on the context.

3. **The role of the 'architect'**: Is the impact intentional (or alternatively, manipulative, coercive, exploitative, strategic, or designed in the provider's interest), or not? We note that the 'architect' in this context refers to the relevant corporate body entity responsible for the architecture, not the individual UX designer within that body.

4. **The nature of harm**: Harmful online choice architecture presumably implies harm, but relative to what counterfactual? It is rare (if ever) that users are fully informed and exhibit complete autonomy. Equally, it is essentially impossible to design a fully neutral online choice architecture. In some cases, a good test may be whether users' choices diverge materially

[18] OECD, 'Dark Commercial Patterns,' 2022.
[19] Mathur, A., M. Kshirsagar and J. Mayer (2021), "What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods", Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, https://doi.org/10.1145/3411764.3445610.

from their underlying preferences? But assessing this may well be unrealistic. Moreover, what about situations where online choice architecture changes those underlying preferences? Or where there are market or societal harms?

While it may be unrealistic to derive a single definition of harmful online choice architecture, we do consider it useful to use consistent terminology and concepts, so far as is possible. However, this is not currently the case across existing EU legislation and guidelines. Taking each of MMK's four elements in turn, we find a wide range of terminology:

1. In relation to **the nature of the online choice architecture**, EU legislation refers to the way providers of online platforms "*design, organise or operate their online interfaces*"[20] and *"the structure, design, function or manner of operation of a user interface or a part thereof*".[21]

2. In relation to **the role of the user interface designer**, they use language such as: *"manipulative",*[22] *"malicious",*[23] *"exploitative",*[24] *"benefit the provider of online platform",*[25] *"subliminal techniques"*.[26] In line with the discussion above, the relevant EU legislation and guidelines are in fact specific that intent is not required (albeit it may be useful evidence of likely effect or a factor relevant to the appropriate remedy). For example, Recital 67 of the DSA defines 'dark patterns' as online interfaces *"that materially distort or impair, <u>either on purpose or in effect</u>, the ability of recipients of the service to make autonomous and informed choices or decisions."* [Authors' underlining].

3. In relation to **the mechanism of the effect on users**, they use terms such as: *"materially distorts or impairs decision-making",*[27] *"materially distorts or is likely to distort behaviour",*[28] *"deceives or manipulates",*[29] *"nudging",*[30] *"presenting choices in a non-neutral manner",*[31] *"subliminal techniques"*[32] or *"causing a person to take a decision that that person would not have otherwise taken".*[33]

4. In relation to **the nature of harm**, they use terms such as: *"users making unintended, unwilling and potentially harmful decisions",*[34] *"not be in the recipients' interests",*[35] *"negative*

[20] Art. 25(1) Digital Markets Act.
[21] Art. 13(6) Digital Markets Act.
[22] Art. 5(1)(a) AI Act; see also Art. 25(1) Digital Services Act ("manipulate").
[23] UCPD Guidance 2021, p. 101.
[24] Recital 67 Digital Services Act.
[25] Recital 67 Digital Services Act.
[26] Art. 5(1)(a) AI Act.
[27] Art. 25(1) Digital Services Act and Recital 67 Digital Services Act.
[28] Art. 5(2)(b) UCPD.
[29] Art. 25(1) Digital Services Act.
[30] UCPD Guidance 2021, p. 101.
[31] Recital 67 Digital Services Act; see also Art. 4(4) Data Act ("offering choices in a non-neutral manner").
[32] Art 5 AI Act
[33] Art. 5(1)(a) AI Act.
[34] EDPB Guidelines 03/2022 on Deceptive design patterns in social media interfaces: how to recognise and avoid them, p. 3
[35] Recital 67 Digital Services Act.

consequences",[36] preventing *"autonomous and informed choices or decisions",*[37] and *"causes or is likely to cause that person, another person, or group of persons, significant harm".*[38]

In addition, where definitions include a variety of these elements, it is also not always clear whether all or just some elements of the definition need to be fulfilled, in order for a practice to be in scope.

We discuss further in Section 2 the issues arising from such a wide range of terminology – and in some cases lack of clarity – especially for effectiveness, consistency across contexts, and the risk of overlap.

1.3 Why Do We Care About Harmful Online Choice Architecture?

The immediate impact of the practices listed above is typically on those making a choice based on online choice architecture. However, the harm arising can in fact be much broader. It can have: [39]

1. **User-level impacts**: Online choice architecture can lead to users making poor choices that do not reflect their underlying preferences. This is directly harmful for those individuals.

2. **Market impacts**: Online choice architecture can lead to users making choices that are harmful for the effective functioning of markets and thus indirectly harmful for people more widely.

3. **Societal impacts**: Users' preferences and behaviour can be influenced over time by online choice architecture in ways that are detrimental for wider societal goals.

Next, we consider each of these categories of impact in more detail.

1.3.1 User-level impacts

The examples of harmful online choice architecture provided above are primarily of interest because they lead to consumers making choices that are not in line with their underlying preferences.

The most commonly discussed harms here are **economic harms** in the context of supplier-consumer relationships. These are a key focus of consumer law. Economic harms can take the form of financial loss, but this is by no means always the case. For example, consumers may be more likely to choose products that are lower quality, or less well suited to their preferences, than they would absent the harmful choice architecture.

In addition, there are a variety of other types of individual harm that are less clearly economic.

- **Time and effort:** For example, if a consumer is able to sign up to a subscription easily, but it takes a long time to unsubscribe, the time and energy taken to unsubscribe is a harm, even if no payment is ever made.
- **Privacy harms:** As a result of online choice architecture in a privacy context, consumers may end up sharing more personal data or allow it to be used more extensively than intended.

[36] Recital 41 Data Act.
[37] Recital 67 Digital Services Act.
[38] Art. 5(1)(a) AI Act.
[39] This analysis draws on the overview of consumer harms in OECD, Dark Commercial Patterns, 2022, pp. 23-28.

- **Violations of autonomy:** Autonomy matters to people in its own right, separately from any resulting outcomes. Brenncke (2023) argues that "regulating dark patterns in European Union law means regulating for autonomy".
- **Psychological harms**: Individuals can also be harmed psychologically when they make poor choices. For instance, they may blame themselves, exhibit stress or depression, or find themselves sucked into addictive behaviour. And of course, these psychological harms can have serious consequential harms for the individual, such as dropping out of school, self-mutilation, or even suicide.

One complexity, though, when talking about underlying preferences, is that people can have time-inconsistent preferences. For instance, when someone clicks onto their preferred social media site, they may only intend to spend five minutes catching up, but can easily get sucked into staying on the site for an hour.

In such circumstances, online choice architecture can help: if the person in question were prompted after 15 minutes of browsing to consider whether they really wanted to continue, they might well opt to leave. However, choice architecture can also exploit such time inconsistency. In particular, there have been significant concerns about **addictive design** online, such as infinite scrolling and auto-play.[40] These may be designed to keep users within a social media service or gaming app, for example, even though – from their own more objective perspective – they would prefer to leave.

1.3.2 Market impacts

If consumers realise they are being deceived or manipulated in particular markets, even if they only do some time later, then they are likely to lose trust in those markets. This will tend to be bad for all concerned, and in particular for those firms that treat their customers fairly. A key role of **consumer policy** is to provide a competitive environment within which fair-dealing firms are not out-competed by those that engage in deceptive or manipulative practices, and thereby help ensure that competition delivers good outcomes.

Over recent years, there has also been increasing focus on online choice architecture within **competition policy**. Competition in markets is fundamentally underpinned by the way in which buyers make choices, and thus online choice architecture which changes consumer choices can naturally also affect competition.

Indeed, there have been a number of antitrust cases relating to online choice architecture. For example, the EU's decision in *Google Android* (2017) addresses abuse of dominance which takes the form of Google using key online choice architecture design elements (defaults) to preference its own services over those of competitors. This in turn prevents competitors from gaining the scale necessary to act as a serious competition constraint on Google's own service, and thus enhances its dominant position.

[40] European Parliament (2024) "Addictive design of online services and consumer protection", https://www.europarl.europa.eu/committees/en/addictive-design-of-online-services-and-/product-details/20230908CDT12141.

Online choice architecture is also relevant to pro-competition regulation, such as the new DMA. As discussed in Fletcher (2024),[41] the DMA has several provisions that relate to online choice architecture, either directly or indirectly, including requirements relating to the easy switching of defaults and the mandatory use of choice screens in certain situations. It also has specific requirements around effectiveness and anti-circumvention, for which online choice architecture is likely to be highly relevant.

1.3.3 Societal impacts

Behavioural science tells us not only that preferences can be time-inconsistent (see above) but that they can also change over time, influenced by experience and context.[42] This in turn means that online choice architecture can have an impact – both positive and negative – in changing the preferences and thus the behaviour of individuals.

On the positive side, online choice architecture can be used to promote a variety of positive changes to individual preferences and thus behaviour, which may in turn have societal benefits, such as within apps that enable users to learn a new language or encourage them to recycle more or take up running or cycling.

However, online choice architecture can also lead to wider societal harm. For example, if individuals feel a loss of autonomy or a lack of control over their environment, they may seek to exert control in other ways, which can lead to broader societal problems.[43]

In the specific context of public discourse, some online content can also be very polarising. If online choice architecture is used to encourage access to such content, for example through the manipulation of what content users see, people may become more extreme in their political views, or more susceptible to believing conspiracy theories, which can in turn lead to a more fragmented, antisocial, and dangerous society, and can even threaten effective democracy.

At the same time, online choice architecture can potentially also be used positively to address such risks. For example, the EU Commission has issued advice that, in order for designated Very Large Online Platforms (VLOPs) and Very Large Search Engines (VLOSEs) to comply with the DSA in the context of elections, they should use *"prompts and nudges urging users to read content and evaluate its accuracy and source before sharing it"*.[44]

[41] Fletcher, A. (2024) "Choice Architecture for end users in the DMA", in de Streel, A., Bourreau, M., Feasey, R., Fletcher, A., Kraemer, J. and Monti, G., Implementing the DMA: Substantive and Procedural Principles, CERRE, http://dx.doi.org/10.2139/ssrn.4700134.

[42] Infante, G., Lecouteux G. and Sugden R. (2016) "Preference purification and the inner rational agent: a critique of the conventional wisdom of behavioural welfare economics," Journal of Economic Methodology, 23:1, 1-25, http://dx.doi.org/10.1080/1350178X.2015.1070527.

[43] Grip. Het maatschappelijk belang van persoonlijke controle | Rapport | WRR.

[44] European Commission, "Guidelines for providers of VLOPs and VLOSEs on the mitigation of systemic risks for electoral processes", https://digital-strategy.ec.europa.eu/en/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes

2. Mapping the EU Regulatory Framework

2.1 Overview of EU Legal Instruments

Several EU legal instruments serve the aim of protecting users from harmful online choice architecture. They differ both in terms of their scope of application and the categories of harms that are being addressed. This section provides a broad overview of the core existing legal framework at EU level.

2.1.1 Unfair Commercial Practices Directive

Probably the most comprehensive piece of EU legislation in this context is the Unfair Commercial Practices Directive 2005/29/EC (UCPD). The UCPD contains no explicit reference to 'dark patterns' or online choice architecture in its articles or in its recitals. This is not surprising, as the term was only coined after the UCPD came into force (see Brignull, 2010). Nevertheless, the Directive with its broad and principle-based provisions appears flexible enough to cover and sanction most categories of harmful online choice architecture.

This view is confirmed by the **UCPD Guidance** of December 2021, which includes a dedicated section explaining how the UCPD applies to 'dark patterns'.[45] According to the Guidance, 'dark patterns' refers to a subcategory of manipulative practices, "*a type of malicious nudging, generally incorporated into digital design interfaces*".[46] As the Guidance explains, such practices can fall under the broad categories of unfair commercial practices addressed in the UCPD. For example, using trick questions and ambiguous language (e.g., double negatives) is likely to qualify as a misleading action under Art. 6 UCPD or a misleading omission under Art. 7 UCPD. Furthermore, using emotion to steer users away from certain choices (e.g., confirmshaming consumers into feeling guilty) could amount to an aggressive practice under Art. 8 UCPD. The Commission's Guidance also underlines that the UCPD does not require intention for the deployment of 'dark patterns'.[47]

In addition, **Annex I** of the UCPD contains a list of those commercial practices that shall in all circumstances be regarded as unfair. With regard to harmful online choice architecture, in particular the following provisions of Annex I are relevant:

- Annex I No. 6: Bait and switch
- Annex I No. 7: False time limited-time statements (e.g., countdown timers)
- Annex I No. 11: Use of editorial content for advertising (e.g., disguised ads)
- Annex I No. 18: Materially inaccurate statements about market conditions (e.g., low-stock messages)

[45] UCPD Guidance 2021, p. 99-102; see also the ACM Guidelines on the protection of the online consumer, March 2023 (providing several examples of how the UCPD applies to the design of online environments).
[46] UCPD Guidance 2021, p. 101.
[47] UCPD Guidance 2021, p. 101.

- Annex I No. 23b, 23c: Social proof
- Annex I No. 26: Persistent and unwanted solicitations ('nagging')

Overall, the UCPD provides a rather flexible framework for addressing harmful online choice architecture on a case-by-case basis. In particular, the general standards of the UCPD provide for "a future-proof 'safety net' and flexibility for consumer authorities and courts to address harmful online choice architecture that evade specific rules".[48]

2.1.2 Digital Services Act

Art. 25(1) DSA prohibits providers of online platforms to "design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions."

As Recital 67 DSA underlines, this provision is aimed at 'dark patterns'. The wording of Art. 25(1) DSA ("**deceives or manipulates**") makes it clear that not only deceptive practices are covered, but also other types of manipulation. In addition, only those practices that "**materially**" distort or impair the decision-making of users are included, i.e., the interference with the decision-making process must exceed a certain threshold. There is a parallel here with Art. 5(2)(b) UCPD which also prohibits a commercial practice only if it "materially distorts or is likely to materially distort the economic behaviour" of an average consumer.

It is important to note that Art. 25(1) DSA not only protects consumers but all "recipients" of the platform services including professional users.

Recital 67 DSA also contains a definition of 'dark patterns' as well as providing several examples:

> *"Dark patterns on online interfaces of online platforms are practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions.*
>
> *"This should include, but not be limited to, exploitative design choices to direct the recipient to actions that benefit the provider of online platforms, but which may not be in the recipients' interests, presenting choices in a non-neutral manner, such as giving more prominence to certain choices through visual, auditory, or other components, when asking the recipient of the service for a decision.*
>
> *"It should also include repeatedly requesting a recipient of the service to make a choice where such a choice has already been made, making the procedure of cancelling a service significantly more cumbersome than signing up to it, or making certain choices more difficult or time-consuming than others, making it unreasonably difficult to discontinue purchases or to sign out from a given online platform allowing consumers to conclude distance contracts with traders, and deceiving the recipients of the service by nudging them into decisions on transactions, or by default settings that are very*

[48] OECD, Dark Commercial Patterns, 2022, p. 40.

difficult to change, and so unreasonably bias the decision making of the recipient of the service…"

According to Art. 25(3) DSA, the Commission may issue guidelines on how Art. 25(1) DSA applies to specific practices. These guidelines should also clarify the relationship between Art. 25 DSA, UCPD and GDPR (cf. Art. 25(2) DSA).

In addition to Art. 25 DSA, which applies to all providers of online platforms, VLOPs and VLOSEs, Art. 34 and 35 DSA are also relevant in relation to online choice architectures. Art. 34(1) DSA requires providers of VLOPs and VLOSEs to diligently identify, analyse, and assess any systemic risks stemming from the design or functioning of their service and related systems or from the use made of their service. The systemic risks to be taken into consideration include serious negative consequences to mental well-being of users (Art. 34(1)(d) DSA). One example could be the use of addictive designs that stimulate behavioural addictions. Art. 35(1) requires VLOPs and VLOSEs to put in place reasonable, proportionate, and effective measures to mitigate systemic risks. Art. 35(1)(a) further specifies that such measures may include "adapting the design, features or functioning of their services, including their online interfaces". In other words, if a harmful online choice architecture leads to systemic risks, Art. 35(1)(a) DSA requires that the user interface design be changed.

2.1.3 Consumer Rights Directive

The Consumer Rights Directive 2011/83/EU (CRD) also contains some provisions that are relevant in relation to harmful online choice architecture.

For example, Art. 22 CRD gives the consumer a right to reimbursement of any "additional payments" for which the consumer's consent was inferred "by using default options which the consumer is required to reject in order to avoid the additional payment". The provision targets a specific category of harmful online choice architecture which exploits default effects ("sneak into basket").[49]

In November 2023, Directive (EU) 2023/2673 added a new Art. 16e to the CRD, which prohibits traders, when concluding financial services contracts at a distance, to design, organise, or operate their online interfaces in a way that deceives or manipulates consumers who are recipients of their service or otherwise materially distorts or impairs their ability to make free and informed decisions. The provision is based almost verbatim on Art. 25 DSA. The provision complements Art. 25 DSA, which only applies to providers of online platforms acting as intermediaries. In contrast, Art. 16e CRD applies to traders who sell their own financial services.

Article 16e CRD is not entirely convincing for several reasons. First, it is somewhat surprising that the scope of application of Art. 16e CRD is limited to financial services. It would have made sense to extend

[49] A similar provision has been introduced in October 2023 by the revised Consumer Credit Directive (EU) 2023/2225. Art. 15 of the Directive stipulates that the agreement of the consumer for the conclusion of any credit agreement or for the purchase of ancillary services must not be inferred through default options (e.g., pre-ticked boxes). See also Art. 23(1) Regulation (EC) No. 1008/2008 on common rules for the operation of air services in the EU which stipulates that "optional price supplements shall be communicated in a clear, transparent and unambiguous way at the start of any booking process and their acceptance by the customer shall be on an 'opt-in' basis."

the provision to all types of consumer contracts covered by the CRD. Second, it seems slightly odd that this provision has been included in the CRD when its more natural place would be in the UCPD.

In the context of "fair design" requirements, the new Art. 11e CRD must also be mentioned. The provision requires traders to prominently display on their online interface a "withdrawal function" which shall be easily accessible to consumers. The provision is a manifestation of an emerging trend towards design-based regulation in EU consumer law. In this sense, Art. 11e CRD underlines that it is not sufficient to grant consumers certain rights (such as the right of withdrawal) and to inform them about their rights (through mandatory disclosures). Rather, the digital environment must also be designed in such a way that it is easy for consumers to exercise their rights – ideally with just one click. Moreover, Art. 11e CRD makes it clear that in some cases it may not be sufficient to outlaw manipulative and deceptive design. Instead, it may be necessary to define positive requirements for "fair design" of user interfaces.

2.1.4 Data Act

The DA of December 2023 also contains specific provisions to protect consumers from 'dark patterns' when making decisions about data access. The provisions shall ensure that users can effectively exercise the rights granted under the DA.

Interestingly, the definition of 'dark patterns' in Recital 41 DA differs from the definition in the DSA: *"Dark patterns are design techniques that push or deceive consumers into decisions that have negative consequences for them*." The phrase "negative consequences" seems overly broad.

The DA contains two provisions that explicitly address online choice architecture. Art. 4(4) DA applies to the relationship between users and data holders, Art. 6(2)(a) DA between users and third parties.

- **Art. 4(4) DA:** "Data holders shall not make the exercise of choices or rights under this Article by the user unduly difficult, including by offering choices to the user in a non-neutral manner or by subverting or impairing the autonomy, decision-making or choices of the user via the structure, design, function or manner of operation of a user digital interface or a part thereof."
- **Art. 6(2)(a) DA:** "The third party shall not make the exercise of choices or rights under Article 5 and this Article by the user unduly difficult, including by offering choices to the user in a non-neutral manner, or by coercing, deceiving or manipulating the user, or by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a user digital interface or a part thereof;"

Both provisions prohibit traders from making "the exercise of choices or rights […] unduly difficult". It is worth noting that the examples of prohibited practices mentioned in both regulations differ. Only Art. 6(2)(a) DA mentions "coercing, deceiving or manipulating the user". Furthermore, the wording differs from Art. 25(1) DSA. It is not clear whether these differences indicate any substantive difference or whether they are merely different paraphrases of the same legal principle.

Another point worth mentioning is that the DA's relationship with the UCPD is organised differently than in the case of the DSA. While Art. 25(1) DSA does not apply to practices "covered" by the UCPD, the DA and the UCPD seem to apply concurrently (see Art. 1(9) DA).

- **Art. 1(9) DA:** "This Regulation complements and is without prejudice to Union law which aims to promote the interests of consumers and ensure a high level of consumer protection, and to protect their health, safety and economic interests, in particular Directives 93/13/EEC, 2005/29/EC and 2011/83/EU."

2.1.5 General Data Protection Regulation

The GDPR contains no explicit reference to harmful online choice architecture. In substance, however, the GDPR contains a number of provisions that can be understood as addressing harmful online choice architecture which incentivise individuals to share their personal data contrary to their preferences.

In February 2023, the European Data Protection Board (EDPB) adopted "Guidelines on deceptive design patterns in social media platform interfaces". The Guidelines provide a number of practical examples of such 'deceptive design patterns' that infringe the requirements of the GDPR that can be applied more broadly than the social media context.

- The first version of the EDPB Guidelines published in March 2022 used the term 'dark patterns'. The final version published in 2023 now refers to the term 'deceptive design patterns'. While the latter term avoids the problematic term 'dark', which may reinforce colourist stereotypes, it is probably too narrow. As discussed in more detail in Section 1, design choices can manipulate users in many ways, not only by "deceiving" them but also by making decisions overly burdensome.
- See the definition of 'deceptive design patterns' in the EDPB Guidelines: *"In the context of these Guidelines, 'deceptive design patterns/ are considered as interfaces and user journeys implemented on social media platforms that attempt to influence users into making unintended, unwilling and potentially harmful decisions, often toward a decision that is against the users' best interests and in favour of the social media platforms interests, regarding the processing of their personal data. Deceptive design patterns aim to influence users' behaviour and can hinder their ability to effectively protect their personal data and make conscious choices."*

A starting point for assessing whether a design pattern infringes the requirements of the GDPR is Art. 5(1)(a) GDPR which stipulates that data must be processed *"lawfully, fairly and in a transparent manner in relation to the data subject"*. In addition, other principles play a role in the assessment of harmful online choice architecture, such as purpose limitation (Art. 5(1)(b) GDPR) and data minimisation (Art. 5(1)(c) GDPR). These principles are further reinforced by Art. 25 GDPR which stipulates that the data controller shall implement technical and organisational measures for ensuring data protection by design and by default.

Furthermore, in 2019 the CJEU[50] ruled in *Planet49* that a pre-ticked checkbox on a website (which the user must actively deselect to refuse consent) does not constitute valid consent under Art. 4(11) and 6(1)(a) GDPR.[51]

[50] Case C-673/17

[51] Wiedemann, K. The ECJ's Decision in "Planet49" (Case C-673/17): A Cookie Monster or Much Ado About Nothing?. International Review of Intellectual Property and Competition Law 51, 543–553 (2020). https://doi.org/10.1007/s40319-020-00927-w

2.1.6 Digital Markets Act

The EU DMA is a regulation specific to a small number of designated big tech 'gatekeeper' platforms. Its objectives are contestability and fairness, albeit 'fairness' here relates to the treatment by these gatekeepers of their business users, not consumers (here termed 'end users').

The DMA is primarily a pro-competitive regulation, with the objective of enhancing market contestability and the fair treatment of business users. However, recognising the importance of consumer decision-making for driving competition, it contains a number of specific requirements that relate to choice architecture. These relate to choice architecture not only on websites but also embedded within devices:

- Under Art. 6(3), certain gatekeepers are mandated to provide consumers with an upfront choice of default search engine and browser. The design of this choice screen has been the subject of much debate (including ongoing), but the clear intention is to open up the search engine and browser markets to increased competition.
- Arts. 6(3), 6(4), 6(6), 6(9), and 6(13) all require that the gatekeepers enable certain user actions (changing of default settings, uninstalling, downloading, switching, data porting, and terminating), and that this should be capable of being done, variously, "easily", "effectively", or "without undue difficulty." Again, the intention of these provisions is to enable rivals to compete more effectively for these users.

In addition, Art. 13 DMA which focuses on anti-circumvention, expressly prohibits any behaviour that undermines effective compliance with the DMA. This prohibits gatekeepers from using interface design to make choices *unduly difficult*, including "by offering choices in a non-neutral manner" or subverting end users' "autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface."

2.1.7 AI Act

The latest addition to the EU regulatory framework on harmful choice architecture is the AI Act. The original proposal of the European Commission envisaged only a prohibition of AI systems that deploy "subliminal techniques beyond a person's consciousness".[52] In the final version of the AIA, the scope of this prohibition has been considerably extended. Article 5(1)(a) AIA now prohibits:

> *"the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of, materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing a person to take a decision that that person would not have otherwise taken in a manner that causes or is likely to cause that person, another person or group of persons significant harm."*

The provision draws attention to the fact that AI systems can be used to deploy new, more sophisticated forms of manipulation, for example through the personalisation of online choice

[52] European Commission, AI Act Proposal, COM(2021) 206 final, Art. 5(1)(a).

architecture ("micro-targeted dark patterns").[53] However, the individual elements of this provision, which has become longer and longer in the course of the legislative process, raise a number of questions. For example, the phrase "purposefully manipulative or deceptive techniques" suggests that the provision presupposes an intention to manipulate or deceive. However, the provision then refers to techniques "with the objective or the effect of materially distorting" the behaviour of a person. The dual expressions "objective" and "effect" seem to indicate that no intention is required with regard to influencing the behaviour of the target group. The question of interpretation becomes even more complicated when Recital 29 of the AIA is taken into account, which states: "In any case, it is not necessary for the provider or the deployer to have the intention to cause significant harm, provided that such harm results from the manipulative or exploitative AI-enabled practices." Does this mean that intention is required regarding the use of manipulative and deceptive techniques but not with regard to the distorting of behaviour and the subsequent harm? Likewise, it is unclear why legislators felt the need to include both a requirement that, in order to be in scope, the practice must "materially distort the behaviour of a person or a group of persons" and that they must, factually, "take a decision that they would not have otherwise taken". It is unclear whether the second limb adds anything or whether it only serves to narrow the potential practices caught within the scope (for example, where the person would have made the same decision in any event). Moreover, Art. 5(1)(a) is rather broad as to the person who suffers harm as a result of the manipulative or deceptive techniques ("*that person, another person or group of persons*"). The broad wording which seems to cover also third-party effects of manipulative techniques raises issues of foreseeability.

2.2 Overlaps and Risks of Inconsistency in the EU Regulatory Framework

2.2.1 Interaction with horizontal law

The brief overview of the current EU regulatory framework for harmful online choice architecture shows that the density of regulation has increased significantly in recent years.

Until a few years ago, the regulation of harmful online choice architecture was essentially based on two pillars: the UCPD in the area of consumer law and the GDPR in the field of privacy law. Both the UCPD and the GDPR contain horizontal regulations that are characterised by broad and principle-based provisions. In the case of the UCPD, these are supplemented by a number of specific prohibitions in Annex I UCPD.

In contrast, the latest layer of regulation at EU level combines various different approaches: On the one hand, the DSA, the DMA, the DA and the recently revised CRD contain specific prohibitions of harmful online choice architecture for certain sectors (distance marketing of financial services), use cases (data access), business models (digital platforms) or categories of businesses (gatekeepers). On the other hand, the AIA adds a prohibition of manipulative and deceptive techniques that applies to a multi-purpose technology that will be widely used across different industries (AI systems).

[53] See Mark Leiser and Christiana Santos, Dark Patterns, Enforcement, and the emerging Digital Design Acquis – Manipulation beneath the Interface, 2023, https://ssrn.com/abstract=4431048; see also Mark Leiser, Psychological Patterns and Article 5 of the AI Act: AI-Powered Deceptive Design in the System Architecture and the User Interface, AIRe 2024, 5 et seq.

This multi-pronged regulatory approach raises the question of how the new sector-specific or technology-specific regulations interact with the existing horizontal regulations and what added value they offer. This question must be answered differently for the various legal acts.

- According to Art. 25(2) DSA, the prohibition of 'dark patterns' in Art. 25(1) shall not apply to practices "covered" by the UCPD or the GDPR. In other words, a business practice that falls within the scope of the UCPD or the GDPR and is lawful under these rules cannot be prohibited under Art. 25(1) DSA.[54] Art. 25(1) DSA remains relevant insofar as a business practice is not covered by the UCPD or the GDPR.
- A relevant scope of application remains for Art. 25 DSA in the following cases in particular:
    - practices towards users who are not consumers;
    - practices that do not directly serve the promotion, sale, or supply of a product to consumers (Art. 2 (d) UCPD);
    - practices that do not influence the economic behaviour of consumers, but rather non-economic activities such as exercising freedom of expression.
- The regulatory landscape becomes even more complex in view of the new Art. 16e CRD, which contains a ban on harmful online choice architecture that only applies to contracts for the distance selling of financial services. The first question that arises here is whether a separate provision is really necessary for the distance selling of financial services. Are there any sector-specific problems here that are not covered by the horizontal regulations of the UCPD? The second question is how the provision interacts with the UCPD. The provision is based almost verbatim on Art. 25(1) DSA. Interestingly, however, Art. 16e CRD does not contain a subsidiarity clause like Art. 25(2) DSA. Instead, Art. 16e is apparently intended to apply alongside the UCPD ("Without prejudice to Directive 2005/29/EC and Regulation (EU) 2016/679..."). It is apparent that, in the area of distance selling of financial services, design choices must therefore comply with both the standard of the UCPD and the standard of Art. 16e CRD. It is unclear why the European legislator has chosen a different model for the interaction of the different regulations than in the case of the DSA.
- Unlike Art. 25 DSA, the provisions prohibiting harmful online choice architecture under the DA do not contain a "subsidiarity clause" that gives priority to the UCPD. Therefore, the UCPD and the DA seem to apply concurrently (see Art. 1(9) DA).

[54] Raue, in: Hofmann/Raue, Digital Services Act, 2023, Art. 25, para. 95.

- The relationship between the AIA and the UCPD is also not entirely clear. Recital 29 AIA merely mentions that the prohibitions in the AIA are "complementary" to the provisions of the UCPD. It is apparently intended that the AIA and the UCPD will apply alongside each other. The AI Act would therefore only have an independent function for practices that are not already covered by the UCPD.
- The fragmented regulatory landscape also raises problems from an enforcement perspective as different authorities are responsible for enforcing the respective regulations. This increases the risk of inconsistencies and legal uncertainty. This is an issue that should be addressed as part of the planned review of the CPC Regulation.

Sector-specific regulations on harmful online choice architecture should only be adopted if they respond specifically to particular problems in a sector that are not covered by the horizontal regulations or if sector-specific regulators are in a better position to enforce the rules or provide guidance to market participants. Duplications and overlaps should be avoided as far as possible. In addition, the European Commission could clarify the interplay between the different regulations on harmful online choice architecture through Guidance Notices, e.g., the next edition of the UCPD Guidance.[55]

2.2.2 The 'average consumer' concept

A controversial question, much discussed in the literature, is whether the benchmark of the **average consumer**, which is a key element of the UCPD, is suitable for addressing harmful online choice architecture, both within UCPD and more widely.

- As set out in Art. 5(2)(b) UCPD, commercial practices must be assessed from the perspective of the "average consumer", "who is reasonably well-informed and reasonably observant and circumspect" (Recital 18). Only in exceptional cases the perspective of a "vulnerable consumer" is taken into account, where a commercial practice targets a "clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product" (Art. 5(3) UCPD).
- Art. 5(3) UCPD refers to intrinsic and permanent characteristics that may make a consumer vulnerable such as "mental or physical infirmity, age or credulity". It has been argued, however, that any consumer can be temporarily vulnerable due to contextual or psychological factors. It is unclear to what extent such a "context-dependent vulnerability"[56] is covered by the UCPD.

[55] Commission Notice, Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market [2021] OJ C526/01.
[56] Lupiáñez-Vaillanueva et al., Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation, April 2022, p. 72.

- Moreover, a growing strand of literature argues that also an average consumer can be considered vulnerable in a digital environment.[57] A study by Helberger et al. (2021) for BEUC coined the term "digital asymmetry" to describe this phenomenon. The authors argue that "[i]n the digital society, vulnerability is architectural because the digital choice architectures we navigate daily are designed to infer or even create vulnerabilities. The vulnerabilities – be they dispositional or occurrent – that consumers can experience are not an unfortunate by-product of digital consumer markets; vulnerabilities are the product of digital consumer markets."[58] Other authors refer to "systemic vulnerability", i.e., a form of vulnerability created by the system design, in particular the design of online choice architectures.[59]

While it is certainly true that the design of online choice architectures can be used to manipulate users, it is doubtful whether a generalisation of the concept of vulnerability is really helpful. If all consumers are vulnerable, the concept of vulnerability loses its distinctive purpose. Instead of expanding the concept of vulnerability, it may be worthwhile to clarify the extent to which the concept of the "average consumer" incorporates behavioural findings. This question is currently the subject of a preliminary reference to the CJEU (Case C-646/22).[60]

[57] See also Zac et al (2023) Dark Patterns and Consumer Vulnerability (arguing that there is "strong evidence that individuals across all groups are susceptible to dark patterns, and only weak evidence that user susceptibility is materially affected by commonly used general proxies for consumer vulnerability").

[58] Helberger et al. (2021) EU Consumer Protection 2.0. Structured asymmetries in digital consumer markets, p. 19; see also Helberger et al. (2024) Digital Fairness for Consumers, p. 12 (explaining that the concept of digital vulnerability is characterised by three aspects, "its relational nature, its architectural nature, and the erosion of privacy").

[59] Riefa (2022), Protecting vulnerable consumers in the digital single market. European Business Law Review, 33, 607-634.

[60] Request for a preliminary ruling from the Consiglio di Stato (Italy) lodged on 13 October 2022 – Compass Banca SpA v Autorità Garante della Concorrenza e del Mercato, Case C-646/22 ("Should the concept of 'average consumer' referred to i Directive 2005/29/EC understood as a consumer who is reasonably well informed and reasonably observant and circumspect — given that it is vague and flexible — be worded according to the best science and experience and thus refer not only to the classic concept of homo economicus, but also to the findings of the latest theories on bounded rationality, which have shown how people often act by limiting the information they need through decisions which appear 'irrational' when compared with those that would be taken by a hypothetically observant and circumspect person; findings that impose a need for greater consumer protection where — as is increasingly the case in modern market dynamics — there is a risk of cognitive influence?"); see also the Opinion of AG Emiliou in the Case C-646/22, 25 April 2024, ECLI:EU:C:2024:367 (arguing that the UCPD "must be interpreted as meaning that the 'average consumer' is not necessarily a rational individual who is proactive in obtaining the relevant information, who rationally processes the information presented to him or her and who is, thus, able to make informed decisions. Whereas, in some situations, the 'average consumer' may be considered as able to act rationally and make an informed decision, the concept is flexible enough for him or her to be perceived, in other situations, as an individual with 'bounded rationality', who acts without obtaining the relevant information or is unable to process rationally the information provided to him or her (including the information which is presented to him or her by the trader)").

3. Ten Principles for Effective Policy for Harmful Online Choice Architecture

The overlaps and risks of inconsistency across the legislation outlined above are a cause for concern. It is unrealistic to rewrite this legislation at his stage, especially since much of it is relatively recent. Nonetheless, we consider it useful to identify **a set of ten core principles for effective policy design and implementation for addressing harmful online choice architecture**. These may inform future legislation, but also feed into guidance and implementation of the legislation already in place.

- **Principle 1:** Do not restrict regulation to only addressing 'intentional' harmful effects.
- **Principle 2:** Regulation should be clear about the 'mechanism of effect on users', but not be restricted only to 'deceptive' online choice architecture.
- **Principle 3:** Regulation should be clear about the nature of the harm involved, and who it pertains to.
- **Principle 4:** Recognise intrinsic limits to informed and autonomous decision-making.
- **Principle 5:** Recognise that context is important for assessing online choice architecture – it can be beneficial as well as harmful, and can be used positively.
- **Principle 6:** Exercise of rights should be easy and not undermined by online choice architecture.
- **Principle 7:** Ensure that regulation addresses online choice architecture across multiple user path elements.
- **Principle 8:** Consider special rules for automated personalised choice architecture.
- **Principle 9:** Behavioural testing should be encouraged, or even required in specific circumstances, and regulators should be able to access test results.
- **Principle 10:** Mitigate risks of regulatory overlap or inconsistency.

Of course, all policy design should seek to be **effective** and **proportionate**, and we take these as core overarching principles for our discussion. Our aim in this section is to identify **additional principles**. Existing EU legislation and guidance in this space already abides by some of these principles, but not all. Indeed, these ten principles may sometimes be in tension with each other and thus may need to be balanced.

Principle 1: Do not restrict regulation to only addressing 'intentional' harmful effects.

As discussed in Section 1, Harry Brignull, the UX expert who coined the term 'dark patterns' refers to 'deceptive patterns' as 'tricks' that firms engage in 'deliberately'. This suggests a requirement of intention. The terminology of 'deception' and 'manipulation' within the DSA arguably also carries an intrinsic element of malign intention.

Nonetheless, **intention is not required for a finding of breach in any of the EU legislation outlined above**. We agree with this approach. A key practical issue with requiring intention for breach is that it can be difficult for a Court or public authority to demonstrate intention. More critically, online choice architecture can be harmful even when that may not be the clear intent of firms.

For example, an airline that offers add-on travel insurance but uses a pre-ticked box in doing so might possibly only intend to encourage consumers to think carefully about such travel insurance. However, for many consumers, we know that powerful default effects result in such pre-ticked boxes leading to unwanted purchases, or at least discouraging shopping around. For this reason, as seen above, such 'opt out selling' is prohibited under EU law.

It could be argued that not incorporating a requirement of intention essentially has the effect of imposing a positive duty on businesses to ensure that their choice architecture is not harmful, an unduly burdensome form of 'fairness by design' requirement. Otherwise, there is a risk that their choice architecture could be found to be harmful, and thus that they are breaching the law, even if this is inadvertent.

Of course, regulators can always seek to overcome this risk through acting proportionally. They will rarely issue a heavy fine in relation to an 'honest mistake', for instance. But this may not be enough. We see three possible further responses to this concern.

1. **There may be some contexts where such a 'fairness by design' requirement does seem proportionate.** For instance, some legislation inherently only applies to large business, such as the DMA (which applies only to a small number of 'gatekeepers') and those elements of the DSA which apply only to 'Very Large Online Platforms and Search Engines' ('VLOPs' and 'VLOSEs'). For these businesses, any harm arising from their online choice architecture is likely to be widespread, and they are also well-resourced to carry out extensive testing of their choice architecture. The risk mitigation requirements within the Art. 35 DSA, which cover the risk of harmful online choice architecture, could be seen as such a requirement.

2. It can also be possible to reduce the burden by setting relatively **specific rules, which firms can simply follow without needing to make any assessment of likely harmful effects**. This might be a good solution where likely harmful effects are easy to foresee, as in the case of pre-ticked boxes. The practices listed within Annex I of the UCPD take this form.

3. For horizontal regulation which affects all firms, but where the effects are more complex, nuanced, and harder to predict, a more proportionate alternative is required. The approach taken in the UCPD has some merit. **Businesses are expected to exercise "professional diligence"**, i.e., "the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity" (Art. 2(h) UCPD). The UCPD guidance[61] further explains that in the context of user interface design the standard of 'reasonable expectations' means that "*traders should*

[61] UCPD Guidance, p.101 (see footnote 55).

take appropriate measures to ensure that the design of their interface does not distort the transactional decisions of consumers."

We would expect 'appropriate' here to allow for proportionality. That is, a trader exhibiting professional diligence would be expected to avoid choice architecture which will have reasonably foreseeable harmful effects, but whether they need to do more will depend on the extent and magnitude of any risk of harm.[62] In this context, we note that none of the other legislation outlined above contains any reference to a concept like 'professional diligence', but such a concept could potentially be incorporated into guidance.

Additionally, we accept that it can be useful when defining harmful online choice architecture to describe it as potentially acting "in a supplier's own interest", as opposed to those of its customers. However, we do not consider it appropriate to restrict regulation to situations where a firm can be shown acting in its own interest. Rather, this can be assumed. We note that this is in line with Recital 67 DSA: *"This should include, but not be limited to, exploitative design choices to direct the recipient to actions that benefit the provider of online platforms, but which may not be in the recipients' interests"* [Authors' underlining].

Principle 2: Regulation should be clear about the 'mechanism of effect on users', but not be restricted only to 'deceptive' online choice architecture.

As discussed in Section 1, existing legislation describes the 'mechanism of effect on users' (MMK, 2021) in a wide variety of ways: *"deceives or manipulates", "misleading", "materially distorts or impairs decision-making", "materially distorts or is likely to distort behaviour", "nudging", "presenting choices in a non-neutral manner", "subliminal techniques",* or *"causing a person to take a decision that that person would not have otherwise taken".*

A first concern with this variety of terms, is that **it is far from obvious how consistent or divergent they are**. For instance, is it possible to identify situations in which online choice architecture might 'materially distort or impair decision-making' but not 'mislead'? Or vice versa? Are any of these concepts a subset of another?

A second concern is whether the right mechanisms are in fact being addressed. As discussed in Section 1.3, we believe **that regulation should not be limited to 'deceptive' online choice architecture**, assuming that 'deceptive' means 'inducing false beliefs.' Online choice architecture can be harmful without any deception occurring. **'Manipulation' is arguably a better term.** It has the benefit that it need not induce any sort of false belief in end users and yet steer them towards harmful outcomes. On the other hand, the word 'manipulation' seems to carry an element of 'intent', which is not in line with Principle 1 above. As such, if this term is used, it is especially important to clarify that intent is not required.

Similarly, we consider that the terms **'misleading'** and **'aggressive',** as used in the UCPD, **may be more able to encompass harmful online choice architecture if they can be interpreted as encompassing**

[62] Art. 5(3) UCPD.

'mis-steering'. There may be merit to clarifying this through guidance, and then potentially using these terms more widely (albeit recognising that the ECJ will have the final word on any legal interpretation).

At the other end of the scale, a third concern is that terms such as **'distortion of behaviour'**, **'causing a decision that a person would not otherwise have taken', or even 'subliminal techniques'** risk being overly broad. Indeed, it could potentially include any sort of online choice architecture, even that which has beneficial effects, such as helpful rankings. As such, this sort of language would ideally only be used alongside a clear description within the legislation of the type of harm to be addressed, as discussed below. Guidance may also have a useful role to play in clarifying what is intended to be addressed by these terms.

Principle 3: Regulation should be clear about the nature of the harm involved, and who it pertains to.

In general, it is helpful if regulation is clear about the nature of harm it seeks to address and who this harm pertains to. However, the regulatory framework outlined above varies in the extent to which it does this.

UCPD

On its face, the UCPD text and associated guidance seem relatively specific both about the nature of the harm involved and who it pertains to. Unless a practice is listed in Annex I, it is only prohibited if it distorts the 'transactional decision' of an 'average consumer' or, as the case may be, a 'vulnerable consumer'.

However, there is some lack of clarity, even in the UCPD. As discussed in Section 2.2.2 above, **it is not currently clear whether the 'average consumer' concept can be assumed to exhibit 'typical' behavioural biases.** We believe that it should, and that this should be clarified in guidance. As discussed above, many behavioural effects result from people's natural use of rules of thumb (or heuristics), given that informed and autonomous decision-making takes extensive time and energy. These cognitive limitations and thus these common behavioural effects are not limited to a subset of vulnerable people (although some people may be particularly affected), but rather are present in all of us.

In our view, the UCPD should provide protection against the exploitation of such effects through harmful online choice architecture. An alternative approach would to be treat all consumers as 'vulnerable', but this would seem to us to devalue the concept of vulnerability. Either way it is important to clarify this issue. Having done so, **we also consider that the 'average person' concept may be useful for other law which relates to the impact of online choice architecture on individuals.**

The UCPD guidance also usefully clarifies that the 'transactional decision' element of the UCPD covers online situations whereby consumers do not make explicit upfront standard cash-based transactional decisions, instead 'paying' for services with their attention or their data.[63] This is important because consumers may not engage with the initial choice made in this context in the same way as they might a pecuniary transaction. However, it is less obvious that the UCPD covers other non-pecuniary harms

[63] UCPD Guidance, page 100.

such as the time or emotional harm associated with a transaction. Since these can be important, **it could usefully be clarified that these non-pecuniary harms are captured, whether through UCPD or Art. 25 DSA.**

Other relevant legislation

Arts. 34 and 35 DSA are also relatively precise about the systemic risks that VLOPs and VLOSEs are expected to mitigate when designing their online interfaces, even if the boundaries of these system risks may be subject to debate and may potentially change over time.

However, some of the other, more recent, legislation discussed above, is less specific about the nature of harm involved. As discussed in Section 1, a variety of harms are mentioned: *"users making unintended, unwilling and potentially harmful decisions", "not be in the recipients' interests", "negative consequences", preventing "autonomous and informed choices or decisions",* leading to *"unwanted behaviour or undesired decisions",* and *"causes or is likely to cause that person, another person, or group of persons, significant harm".*

A potential concern about several of these is that the nature of the harm involved appears broad and, as highlighted in the previous section, potentially overlapping. **It would be useful to see the development of guidance over time that provides more clarity as to the nature of the harm that is covered under each law.** Where there is an absence of established ECJ case precedent, this may require the Commission to interpret the law on the basis of anticipating undecided situations. As above for UCPD, it should also be clarified to what extent non-economic harm, in particular psychological harm, is covered by the legislation.

There is also substantial variation across this new legislation in terms of who the harm should pertain to. To some extent this is appropriate given the differing aims of the legislation. UCPD is clearly limited to the protection of natural persons in their role as consumers. But in the context of platforms, individuals are also affected as 'people' or 'citizens'. Business users too are also a type of customer and, while these can range from huge corporations to individuals selling via an online marketplace, there may be situations in which their decision-making too is affected by choice architecture. We note that the other regulations outlined above are more general.

For example, the Art. 25 DSA, which is applicable to all online platforms (and not just very large ones), covers '**recipients'** of the online choice architecture. This could presumably include both individual citizens[64] and businesses. The DSA and AIA also address wider societal effects. In the DMA, the harm involved is not related to individuals at all (other than indirectly), but rather the impact that ineffective user decision-making can have on contestability and fairness (where 'fairness' here relates to fair treatment of businesses, not consumers).

However, while these extensions have some value, there may also be risks to such a broad scope of application. For example, Art. 5 of the AIA refers to resulting harm to "*that person, another person, or group of persons".* This gives rise to a risk – especially when combined with other elements in this Article – that this effectively overlaps with several other laws.

[64] To the extent that they are not excluded from the scope of Art. 25(1) by virtue of Art. 25(2).

Principle 4: Recognise intrinsic limits to informed and autonomous decision-making.

We spoke above about the need to allow for behavioural effects within the 'average consumer' context, but the prevalence of behavioural effects has further implications too.

First, it is relevant to **any elements of the law which are effectively predicated on a counterfactual of fully informed individuals, who exhibit complete autonomy, and a fully neutral choice architecture.** Some of the legislation outlined in this report has a flavour of this. For example, Article 4(1)(d) of the DA prohibits data holders from making *"the exercise of the rights or choices of users unduly difficult, including by offering choices to the users in a non-neutral manner or by subverting or impair the autonomy, decision-making or free choices of the user."* [Authors' underlining]

Second, **just because information has been provided, does not mean that individuals necessarily take it into account in the way intended.** For instance, even if something has been presented in apparently 'plain and intelligible' language, this does not necessarily mean that a typical consumer would understand it. If one takes typical cognitive limitations seriously, it may be possible to provide information in ways that are easier to digest. This is relevant to the Unfair Terms in Consumer Contracts Regulations (UTCCRs, 1999CRD.). Interpretation of this law could usefully give greater weight to whether the language provided enables effective decision-making in practice. Likewise, the UCPD requirement that marketing communications could be clearly labelled as such could usefully give greater weight to whether users observe and understand such labelling.

In some circumstances, information requirements may be completely ineffective, or even have unintended negative consequences. A recent example is the mandatory disclosure of personalised pricing resulting from the 2019 Modernisation Directive (2019/2161), amending the CRD. It is not clear how consumers are expected to deal with the disclosed information, and there is even evidence that such disclosure can be framed in such a way that it worsens consumer choices.[65] In such cases, legislation may need to be strengthened if it is to be effective.

Third, in some contexts, it may be **useful to introduce small frictions to encourage people to engage in greater deliberation**, for example by removing 'ticks' from previously pre-ticked boxes (as required under the CRD) or introducing search engine and browser choice screens (as required under the DMA).

We note, though, there are also costs to such interventions, and thus such interventions need to be employed with care. For example, the benefits of introducing small frictions need to be balanced against the fact that **users tend to value a smooth journey through a set of choices**. Likewise, if consumers are required to make too many choices, they may exhibit choice fatigue, and thus either put off making decisions or make them quickly, potentially worsening the behavioural effects described above and the risk of bad outcomes. As mentioned above, this has been a concern in relation to the cookie consents required under the ePrivacy Directive.

[65] van Boom, W.H., van der Rest, JP.I., van den Bos, K. et al. (2020) "Consumers Beware: Online Personalized Pricing in Action! How the Framing of a Mandated Discriminatory Pricing Disclosure Influences Intention to Purchase." *Social Justice Research* 33, 331–351. https://doi.org/10.1007/s11211-020-00348-7.

The EU DMA arguably strikes **a good balance between adding frictions sparingly, while allowing consumers generally the benefit of a smooth journey**. Recognising the positive impact that default settings can bring, in terms of not having to keep making repeated decisions, the DMA does not prohibit them. Rather Art. 6(3) DMA requires that end users should be given an upfront choice of default search engine and browser only in very specific circumstances (that is, for designated browsers which would otherwise use their proprietary search engine), and thereafter that it should be easier for them to change this default setting if they so wish.

Principle 5: Recognise that context is important for assessing online choice architecture – it can be beneficial as well as harmful, and can be used positively.

As is clear from the above discussion, context matters for the assessment of choice architecture, and it can be used in beneficial ways, as well as harmful ones.

This has two important implications.

First, **policy intervention should seek to avoid discouraging online choice architecture that is intended, and likely, to be beneficial to recipients.** It would not be a good outcome, for example, if online marketplaces were deterred from using choice architecture that encourages price comparisons across products, or if ecosystems were deterred from offering any default apps.

We recognise, however, that – as with many areas of policy – there may be a tension here between getting the right answer in every case and setting specific rules. In principle, it might seem best to consider all harmful online choice architecture based on its outcomes, but this is unlikely to provide much-needed legal certainty and easy compliance for firms, and clear expectations for users.

As mentioned above, one way around this tension is to set specific rules for the most obviously harmful online choice architecture, as in Annex I of the UCPD. In this context, we note that recent work by the UK Competition and Markets Authority,[66] as shown in Table 1 below, has sought to distinguish between those online choice architecture practices that are highly likely to be harmful (marked with *), and those where the overall effect will depend on the precise context in which they are used. However, this work is very preliminary. We note that the empirical literature in this area is growing fast, and regulators could usefully encourage it to grow faster.[67]

[66] See footnote 3.

[67] Singh et al (2023) apply a somewhat more formalised methodology to the same task. They categorise a variety of 'dark patterns' into 6 overarching buckets and used formalised surveys with industry experts to identify their relative importance in the e-commerce industry. The bucket they identify as being most important is the one they call 'exigency' which comprises urgency messages of various sorts (low-stock messages, high-demand messages, limited-time messages, countdown timers). The second most important bucket was 'social proof', which included fake user activity or fake endorsements but also 'toying with consumers' emotions. This type of analysis has potential to contribute empirical support for the development of further Annex I banned practices, albeit it should not be relied on alone – actual behavioural experiments provide far stronger evidence.

Table 1: A taxonomy of OCA practices

Choice structure	Choice information	Choice pressure
Defaults Ranking Partitioned pricing Bundling Choice overload and decoys* Sensory manipulation* Sludge* Dark nudge* Virtual currencies in gaming Forced outcomes*	Drip pricing* Reference pricing Framing Complex language* Information overload*	Scarcity and popularity claims Prompts and reminders Messengers Commitment Feedback Personalisation

We note, though, that the UCPD is currently the only law relating to online choice architecture that includes such a 'prohibited list' of practices. The other legislation mentioned above is more general and outcome focussed. This means, unless implemented and enforced carefully**, it does risk creating precedents that deter positive online choice architecture.** There may therefore be merit in employing a similar 'banned practices' approach for regulation beyond UCPD, to the extent that this can be done through guidance.

Second, in certain circumstances**, it may be appropriate for policy makers to impose positive regulatory requirements in relation to online choice architecture**, as opposed to simply imposing prohibitions. Countering harm by enabling choices that are better aligned with preferences.

Such positive requirements can potentially result from the enforcement of law that is itself based on prohibitions. For example, to meet its obligations under UCPD, one subscription service has recently committed to enabling EU/EEA consumers to unsubscribe with just two clicks, using a prominent and clear 'cancel button'.[68]

Alternatively, in certain contexts, positive requirements can usefully be incorporated within legislation. For instance, the Art. 6(3) DMA requirement for an upfront choice of default search engine and browser is specifically intended to promote fairness and contestability in search in the context of one firm holding a near-monopoly. Art. 6(4), which enables third party apps to prompt users to make them their default, has the same intent but potentially across a wider range of services. Where appropriate, **such positive requirements could usefully include prescriptive design rules, such as a standardised cancellation button.** Of course, any such positive requirement would need to be carefully assessed for effectiveness and proportionality, which would include considering possible side-effects.

In such circumstances, as discussed in Fletcher (2024)[69], there may even be a need to impose choice architecture that does not fully reflect underlying user preferences.

[68] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_4186.

[69] Fletcher, A (2024) "Choice Architecture for End Users in the DMA", chapter in De Streel et al (2024*) Implementing the DMA: Substantive and Procedural Principles*, CERRE Report, https://cerre.eu/wp-content/uploads/2024/01/CERRE-BOOK-IMPLEMENTINGDMA.pdf.

- For instance, fairness and contestability are unlikely to be best achieved by including the current near-monopolist at the top of the choice screen, even if this ranking would arguably reflect end users' current underlying preferences.
- For competition reasons, therefore, it would be better to downrank this service, albeit without doing so to such an extent that end user autonomy (the ability to choose Google if they so wish) is undermined.

Principle 6: Exercise of rights should be easy and not undermined by online choice architecture.

With enhanced understanding of behavioural science, it should be clear that it will not always be sufficient to give users legal rights, or even to inform them about those rights. As argued by Micklitz et al (2024),[70] consumers will struggle to utilise these rights, especially in a complex digital environment. Thus, **it is critical that exercise of those rights should be easy, and not undermined by online choice architecture**.[71]

A positive example here is the DMA which requires not only that end users should have the right to take a set of specified actions (uninstall or switch apps, change default settings, download apps and app stores from the web), but also that these actions should be easy. The same is true of the DA which, as well as conferring the rights for users to access (Art. 4) and share (Art. 5) data linked to connected products, it is made explicit that these rights should be easy to use, and not made unduly difficult through interface design.

The clear and prominent 'cancel' button mentioned above is another example, as is the recently introduced Art. 11a CRD which requires traders to prominently display on their online interface a 'withdrawal button' which shall be easily accessible to the consumer.

Of course, this raises questions of 'how easy is "easy,"' and 'how can compliance be demonstrated'. In general, fewer steps will tend to be easier than more. As such, 'deeplinks' – which take users to specific settings within a website, app, or device – can be useful. However, greater precision could again be provided through guidance.

We also note that **there are a wider range of regulations, potentially extending beyond those discussed above, where choice architecture could be a way of circumventing the law.** For example, any law that requires a choice to be offered can potentially be stymied if that choice is made hard to find, hard to understand, or hard to act on.

The DMA is alert to this issue; Art. 13(6) states:

> *"The gatekeeper shall not […] make the exercise of th[e]se rights or choices unduly difficult, including by offering choices to the end-user in a non-neutral manner, or by subverting end users' or business users' autonomy, decision-making, or free choice via*

[70] Hans-W. Micklitz et al (2024), 'Towards Digital Fairness,' 13 *Journal of European Consumer and Market Law* 24. https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/13.2/EuCML2024004.

[71] See also Autoriteit Consument & Markt, EU Fitness Check on Digital Fairness: Protecting Consumers in Digital Environments, November 2022.

the structure, design, function or manner of operation of a user interface or a part thereof."

We believe the EU should consider the more extensive use of this sort of anti-circumvention clause across other legislation.

Principle 7: Ensure that regulation addresses online choice architecture across multiple user path elements.

A key finding of behavioural science is that there can be important interactions between different stages of a person's decision-making journey, or 'user path'. **The timing, context, and number of user path elements can also have a substantial impact.**

For example, are users even informed that there are choices that can be made? Are they asked to make a choice at a time it seems relevant, or in the middle of an unrelated workflow? Before making a choice, are users given relevant context such as: 'The EU has decided that users should be given more choice about their default search engine. The following choice screen is designed to give you that choice.'? Are users able to go back a stage easily, without being thrown out of the user path, and having to start again? Are users able to reverse their decision at a later stage, and – if so – are they told this? Are users shown 'scare screens' intended to deter them from a particular action? People may also react differently within voice-only or virtual reality interfaces than they do in a standard screen-based environment.

This means that it is important to consider the overall system architecture relating to user choice, and not just the design of any specific interface. There can also be 'system level' dark patterns, resulting from basic system design. However, **much of the legislation described above refers only to 'interface design'. It would be useful to clarify that this term can encompass multiple user path elements.**[72]

In considering these various user path elements, it can sometimes be useful to consider the various steps that can be involved in any given decision-making process. For example, in a consumer transaction, the decision-making process frequently comprises four distinct steps (sometimes known as the 4 As of decision-making):[73]

1. ***Attending*** to the decision in the first place. For example, users may need to be encouraged, or even required, to engage. Small frictions such as prompts or choice screens can be useful in this context.

2. **Accessing** relevant information about the available options. Access should be easy and the information should be well-designed to enable effective decision-making.

[72] A similar argument is made in Leiser, Dr Mark and Santos, Dr Cristiana, Dark Patterns, Enforcement, and the emerging Digital Design Acquis: Manipulation beneath the Interface (April 27, 2023). Available at SSRN: https://ssrn.com/abstract=4431048.

[73] Fletcher, A. (2021) "Disclosure as a tool for enhancing consumer engagement and competition," *Behavioural Public Policy*. 2021;5(2):252-278, https://doi.org/10.1017/bpp.2019.28.

3. **Assessing** those options. Options should be presented either in a way that supports easy comparison, and the choice architecture should either be aligned to user preferences or be as neutral as possible.

4. **Acting** on that assessment. While some friction can be useful for encouraging deliberation, users should not face unnecessary frictions, such as multiple clicks or scare screens, that might unduly deter them from acting. The ability to reverse a decision, sometimes in the form of a cooling-off period, can also be valuable for encouraging action.

In addition, the supplier-user relationship in digital environments often goes beyond the initial transaction. For example, in subscription contracts, there may be a variety of choices that a user can make over time, including continuing with the service, using it more (or less), or cancelling it. Consumers may not 'attend' to these ongoing choices and find themselves paying for services they don't use or facing an unduly high price. Even if they do attend to the issue, they may struggle to access relevant information, assess it, or act on it. Subscriptions with initial free or discounted periods can be especially problematic in this regard.

Improving the online choice architecture associated with such ongoing relationships has the potential to enable better decision-making, but **this would require specific requirements in consumer protection law.**

Principle 8: Consider special rules for automated personalised choice architecture.

While the behavioural effects outlined above apply to everyone, it remains true that individuals may exhibit different biases to differing extents, that this impact may also vary across different contexts or in differing emotional states. This means that **there is potential to design online choice architecture algorithmically, on a personalised basis, to reflect the specific biases of individuals or of groups of individuals with similar characteristics.** This is facilitated online by the potential for online firms both to collect extensive personal data and to carry out extensive online testing of different choice architecture designs.

Such personalised choice architecture can potentially be beneficial, providing targeted help for individuals facing complex decisions, or helping to make consumers aware of products that will suit them. However, it can also be harmful. Helberger et al (2021)[74] argue that it can also be used to create make any consumer vulnerable. By using personal data to create 'persuasion profiles,' **suppliers can design personalised choice architecture which is especially well-designed to achieve harmful effects for specific individuals or groups of individuals.**

Such harmful personalised online choice architecture is difficult to police. Unless users are carefully taking screen shots of their journey (which is unlikely), it may be almost impossible to demonstrate what choice architecture they faced. Indeed, since harmful choice architecture is frequently, by its nature, hidden, individual consumers may well not even realise they have experienced it. This

[74] Helberger, N., Sax, M., Strycharz, J. et al. (2022) "Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability," Journal of Consumer Policy, Vol 45, 175–200. https://doi.org/10.1007/s10603-021-09500-5.

provability issue will be exacerbated due to the involvement of algorithms or other forms of automation in the choice architecture design process. There may even be instances where even the supplier involved may not know how a choice was presented on any specific occasion, for example, if an algorithm or automated design solution determined the approach.

For this reason, **there may be merit in imposing relatively strong rules in relation to automated personalised online choice architecture.** For example: personalisation on the basis of restricted characteristics or emotional state could simply be banned; and any firms wishing to use automated systems to deliver personalised online choice architecture could have a 'duty of care' to test their systems and ensure they are 'fair by design'.

However, we note that any such rules should, if possible, seek to ensure that beneficial personalisation is not unduly deterred, which may be a delicate balancing act.

Principle 9: Behavioural testing should be encouraged, or even required in specific circumstances, and regulators should be able to access test results.

Although there is extensive evidence on the common behavioural biases described above, it can still be hard to predict how specific instances of online choice architecture will affect user choices.

For this reason, **if firms are to be sure that their designs do not have harmful effects, this may need to be tested empirically.** Indeed, many online firms anyway already engage in extensive empirical testing, often in the form of 'A/B testing', which compares the effects of two alternative designs on user choices. Such testing can be carried out repeatedly, to test a whole series of design options.

For instance, in the context of its search function, Google emphasises that it does "*hundreds of thousands of quality tests and experiments to figure out how to make Google more helpful for you. Many of these ideas don't pan out, but some do, and it's through experimentation that Search gets better.*"[75]

Of course, such testing can play an important and beneficial role in the design of online choice architecture. But it can also be useful for identifying harmful online choice architecture. That said, A/B testing may not be sufficient on its own to assess whether choice architecture is harmful; it only demonstrates the impact of different designs on user choices, not whether those choices are good ones, or whether they reflect the users' underlying preferences. There may, therefore, be value in supplementing such testing with short surveys, which take place immediately after the choice has been made. For example, these could be designed to ascertain whether the user has understood the options that were available, and whether they are content with their choice.

We discussed above the situations in which it is likely to be proportionate to require firms, on an ongoing basis, to positively ensure that their online choice architecture is not giving rise to harmful effects. For example, this is clearly required of VLOPs and VLOSEs under the DSA. **Where this is the case, we might expect such empirical testing to be utilised**. **It would also seem reasonable to require firms to ensure that any such testing results are captured and retained within the firm, so that they**

[75] https://blog.google/products/search/search-labs-ai-announcement-/

are available for later authority review. We note that Art. 34(3) DSA requires this of VLOPs and VLOSEs in the context of the testing they carry out to assess systemic risk.

More generally, across the legislation outlined above, we would suggest that authorities and courts, when assessing the impact of specific online choice architectures, **should have the right to request access to past testing data (where available) and even to require empirical tests to be carried out (where proportionate).** Such testing may be especially important when designing interventions, to confirm that a proposed intervention is indeed likely to be effective at solving the issue at hand. We note that Art. 40 DSA requires VLOPs and VLOSEs, likewise, that VLOPs and VLOSEs "*shall provide the Digital Services Coordinator of establishment or the Commission, at their reasoned request and within a reasonable period specified in that request, access to data that are necessary to monitor and assess compliance with this Regulation*."

In addition, under the DSA, there is the potential for vetted researchers to access and analyse the resulting data. **This is a new approach that could usefully be considered within other legislation**.

Authorities should have regard to online behavioural experiments – such as those carried out by Mozilla[76] and BEUC[77] in the context of the DMA – and may even wish to commission or carry out such experiments, either alone or alongside businesses.[78]

In addition, we recommend that **authorities should consider hiring experts in behavioural science and UX design** to enhance their review – and any commissioning – of all types of choice architecture research.

Finally, we note that authorities are increasingly using 'behavioural audits' where they do searches for particular elements of online choice architecture known as likely to be harmful.[79] Firms, too, may find such behavioural audits useful, for ensuring that their own online business does not incorporate any likely harmful choice architecture.

Principle 10: Mitigate risks of regulatory overlap or inconsistency.

An important policy question is the extent to which regulation should be aligned across the online and offline environments, and the extent to which regulation should be different online, to address the specific issues arising in a targeted way. We note that some of the regulation outline above (such as the UCPD) applies equally in both environments, albeit its implementation may be subtly different. However, other regulations (such as the DSA, DMA, and AIA) clearly relate to the online environment.

[76] Mozilla (2023) *Can browser choice screens be effective?,* available at: https://research.mozilla.org/browser-competition/choicescreen/.

[77] BEUC (2023) *An Effective Choice Screen under the Digital Markets Act*, available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-131_An_effective_choice_screen_under_the_DMA.pdf

[78] For example, Effective online information: Studies into the improvement of online disclosures for consumers | ACM.nl.

[79] See: Mills, S. *et al.* (2023) "Dark patterns and sludge audits: an integrated approach", *Behavioural Public Policy*, pp. 1–27. doi:10.1017/bpp.2023.24; and Behavioural Insights Team (2022) "Behavioural Risk Audit of Gambling Operator Platforms", https://www.bi.team/wp-content/uploads/2022/07/Behavioural-Risk-Audit-of-Gambling-Operator-Platforms-findings-report-July-2022.pdf

We consider this a complex issue, where context will be important. On the one hand, **the issues arising from choice architecture tend to be amplified in an online environment, which might merit targeted regulation, but equally it is important that regulation doesn't unduly favour either offline or online channels, so far as is possible**.

In the previous section, we identified several areas of potential regulatory overlap and risks of inconsistency. This creates a number of concerns. Where terminology varies across legislation, **it becomes harder to utilise legal precedent generated under one law to help interpret rules within another.** Where there are overlaps, there are also **risks of double jeopardy**. Where there are carve outs – such as the carve out within Art. 25 DSA of practices covered by the UCPD and the GDPR – **any ambiguities related to the scope of one law can create associated ambiguities around the scope of another.**

For this reason, we would recommend that **any further legislation takes care to utilise consistent terms where possible, but also that guidance is used to clarify the intended links between terms and the legislative provisions themselves.**

We also note that all of these issues are further exacerbated by the fact that much of the legislation outlined above has different enforcement mechanisms, potentially involving different authorities or courts. This increases the **need for effective cross-regulator liaison and enforcement**. The European Competition Network (ECN), and Consumer Protection Cooperation (CPC) Networks – which link relevant authorities across Member States and Brussels – provide one possible approach to this. The UK's Digital Regulation Cooperation Forum – which links domestic regulators with a particular interest in digital markets issues – is another.[80]

[80] https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum.

4. Summary of Recommendations

In Section 3, we highlighted ten principles that could usefully be employed by policymakers when designing and implementing legislation relating to online choice architecture. Our core recommendation in this report is that policy makers adopt these principles, noting that they may sometimes be in tension and thus balancing may be required.

In addition, though, we have also highlighted throughout Section 3 several more specific and actionable recommendations for EU policy makers. These arise from considering these principles. The recommendations, which can be clustered around six overarching themes, are summarised below:

Terminology

1. Drop use of the 'dark patterns' terminology. Consider using 'harmful online choice architecture'.

2. Confirm through guidance that the terms 'misleading' and 'aggressive' as used in the UCPD encompass 'mis-steering', and then consider using these terms more widely.

3. Ensure that any further legislation takes care to utilise consistent terms where possible and use guidance to clarify the intended links between existing terms and legislative instruments.

Average consumer concept

4. Confirm through guidance that the 'average consumer' concept in UCPD allows for 'typical' behavioural effects. Consider drawing on this concept for other law which refers to effects on individuals.

5. Clarify through guidance that legislation is not predicated on a counterfactual world within which individuals are fully informed, exhibit complete autonomy, and within which online choice architecture is fully neutral.

6. Clarify that requirements for 'plain and intelligible' language in the UTCCRs CRD and for clear labelling of advertising in UCPD should make allowance for typical cognitive limitations.

Categories of harm

7. Beyond UCPD, provide clarity, through guidance, as to the nature of the harm that is covered under each law.

8. Confirm through guidance the extent to which non-pecuniary harmful effects of online choice architecture are covered by each relevant piece of legislation.

Positive use of online choice architecture

9. Consider the use of positive regulatory requirements in relation to online choice architecture, not just prohibitions. These could include prescriptive design requirements, such as standardised cancellation buttons.

10. Consider regulation that introduces or facilitates 'small frictions' to encourage greater deliberation.

11. Ensure that exercise of legal rights is easy, and not undermined by online choice architecture.

Targeted changes to consumer protection regulation

12. Draw on the fast-emerging literature on harmful choice architecture to consider candidates for additional Annex I UCPD banned practices. Consider employing a similar 'banned practices' approach for targeted regulation, beyond UCPD.

13. Consumer protection law should provide specific provisions for ongoing supplier-consumer relationships, such as subscriptions.

14. Consider relatively strong regulation for algorithmically personalised online choice architecture.

Compliance and enforcement

15. Consider introducing anti-circumvention requirements relating to online choice architecture to a wider range of regulations.

16. Where large online firms face specific requirements relating to choice architecture, as under the DMA and Art. 35 DSA, they should be expected to carry out empirical testing of key design decisions, and ensure that the data are captured and retained, so that they can be made available for later authority review.

17. More generally, authorities and courts involved in enforcing regulation relating to harmful online choice architecture should have the right to request access to past testing data (where available) and to require empirical tests to be carried out (where proportionate).

18. The 'vetted researcher' provisions of the DSA, which enable vetted experts to analyse data provided to the regulator, are potentially useful and could be considered within other legislation.

19. Authorities should consider hiring experts in behavioural science and UX design to review, and potentially commission, behavioural testing research.

20. Ensure effective cross-regulator liaison and enforcement for authorities involved in enforcing the various regulations relating to harmful online choice architecture.

cerre Centre on Regulation in Europe

Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu

Centre on Regulation in Europe (CERRE)
CERRE Think Tank