OECD*publishing*

DARK COMMERCIAL PATTERNS

OECD DIGITAL ECONOMY PAPERS

October 2022 **No. 336**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

There is mounting concern that dark commercial patterns may cause substantial consumer detriment. These practices, which are commonly found in online user interfaces, steer, deceive, coerce, or manipulate consumers into making choices that often are not in their best interests. In light of the growing need to address dark commercial patterns comprehensively, the OECD Committee on Consumer Policy first held a roundtable on the topic in November 2020 (OECD, 2021[9]). This report builds on the roundtable discussion, in particular by proposing a working definition of dark commercial patterns, setting out evidence of their prevalence and harms, and identifying possible policy and enforcement responses to assist consumer policy makers and authorities in addressing them. It also documents possible approaches consumers and businesses may take to mitigate dark commercial patterns.

The report was prepared by Nicholas McSpedden-Brown, under the supervision of Brigitte Acoca of the OECD Secretariat and in consultation with the Committee on Consumer Policy's advisory group on dark commercial patterns. It was approved and declassified by written procedure by the Committee on Consumer Policy on 24 August 2022 and prepared for publication by the OECD Secretariat.

Note to Delegations:

This document is also available on O.N.E under the reference code:

DSTI/CP(2021)12/FINAL

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Table of contents

Executive summary

The term “dark (commercial)[1] patterns” refers to a wide variety of practices commonly found in online user interfaces that lead consumers to make choices that may not be in their best interests, including by exploiting consumer biases. They typically seek to get consumers to give up more money, personal data or attention time than desired. In this way, they are inextricably linked to an underlying business model, even if user interface designers may often bear no malicious intent.

The OECD Committee on Consumer Policy proposes a working definition of dark patterns to facilitate near-term discussion among regulators and policy makers across jurisdictions: *“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.”* The full definition appropriate in a particular setting may depend on its intended use and the broader policy, legal or technological context.

Many e-commerce[2] websites and apps, including those of major online platforms, feature more than one dark pattern. Online games, browsers, and many cookie consent notices also commonly feature them – the latter potentially entailing high rates of data protection law violation. The more frequent dark patterns on websites and apps involve framing (preselecting choices by default or giving them visual precedence, hiding information or disguising advertisements); creating a sense of urgency (through potentially misleading scarcity indications); generating social proof (through potentially misleading popularity indications); forcing registration or information disclosure; nagging to make a choice; or making it difficult to cancel or opt out.

Given online businesses’ ability to repeatedly run experiments to hone user interfaces, consumers’ heightened susceptibility to deception online and the scale of consumers reachable, dark patterns are likely a greater concern than analogous practices offline. Indeed they can influence consumer decision-making substantially. They appear more effective on mobile devices and when combined. Some, such as hidden information, appear substantially more effective than others, such as scarcity cues. Seemingly mild dark patterns, such as preselecting choices and making it hard to decline, may be as or more effective than aggressive ones such as nagging and toying with emotions. A dark pattern’s effectiveness may in part be driven by the difficulty in its detection, which may relate to whether consumers have prior experience with it, its intrinsic subtlety or general pervasiveness.

In addition to impairing autonomy, some dark patterns, such as drip pricing and subscription traps, can cause substantial financial loss. Others may cause significant privacy harms or psychological detriment. They may also harm consumers collectively, by weakening competition and sowing distrust, and can disproportionately harm certain consumers such as less educated consumers or children. While there is not yet evidence suggesting that dark patterns triggering personal vulnerabilities are common, this may change with businesses’ increasing data collection combined with machine learning techniques.

Market forces are unlikely to address dark patterns alone, and may at times incentivise their use. Consumer and data protection authorities have accordingly been taking action on the basis of laws outlawing practices associated with many dark patterns, while also issuing guidance to support business compliance. But enforcement cases to date predominantly relate to a few dark patterns commonly recognised by regulators, which could point to gaps in the law, in available evidence, or in enforcement capacity. In particular, some dark patterns are not clearly deceptive and may evade prohibitions on deceptive practices.

Various regulatory measures to respond to dark patterns have been proposed or implemented across OECD jurisdictions. These include measures to address them specifically on online platforms; prohibit specific

dark patterns; foster consumer-friendly choice architecture (e.g. by making it as easy to cancel as to sign up); empower regulators; and address consumer vulnerability. However, much evidence indicates that disclosure and transparency measures are insufficient in isolation. Other key considerations relate to combining principle- and rule-based consumer laws; employing specific tools to gather evidence (e.g. web scraping); enhancing co-operation among policy areas (e.g. privacy, artificial intelligence and competition policy); and adapting the interpretation of legal standards.

Initial evidence of dark patterns' prevalence, effectiveness and harms provides directions for possible further action, such as focusing on dark patterns on mobile devices and popular websites. Given dark patterns specifically involving hiding information, making it hard to cancel or opt out, preselecting choices or giving them visual precedence are effective, highly prevalent (on websites and apps, including of major online platforms, and cookie notices) and hard for consumers to detect, they could be a priority focus. Overall, however, more evidence is needed regarding many dark patterns to further guide policy and enforcement efforts.

Technical tools, such as browser extensions, may also help consumers mitigate dark patterns and other measures can raise awareness about them, such as information campaigns. Various business initiatives may also assist, including self- or co-regulatory initiatives, ethical design standards, and digital choice architecture self-audits. While such tools and initiatives can play an important supporting role, they should be seen as complementary to robust regulatory and enforcement measures.

1. Introduction

There is mounting concern that dark commercial patterns may cause substantial consumer detriment. These practices are commonly found in online user interfaces and steer, deceive, coerce or manipulate consumers into making choices that often are not in their best interests.

While the term is relatively new, a number of the practices it encompasses have long been employed by businesses and marketers and scrutinised by behavioural scientists and legal scholars, and have been actionable under existing laws. The OECD Committee on Consumer Policy (CCP) has at various times conducted work on specific online commercial practices that have been classified as dark patterns. These include drip pricing, subscription traps, disguised advertisements and misleading data practices (OECD, 2019[1]; OECD, 2019[2]; OECD, 2019[3]; OECD, 2019[4]). The CCP has also raised awareness of the role of cognitive and behavioural biases with regard to such practices (OECD, 2018[5]; OECD, 2010[6]; OECD, 2017[7]). Other OECD reports have examined the role of machine learning algorithms in marketing and advertising (OECD, 2019[8]).

Nonetheless, research that considers the broad spectrum of dark patterns and their associated harms has only emerged more recently and is mostly from academia. Moreover, even where there is evidence of consumer detriment, some dark patterns may fall outside of the scope of existing regulatory frameworks.

In light of the growing need to address dark patterns comprehensively, the CCP first held a roundtable on the topic in November 2020 (OECD, 2021[9]). At the event, stakeholders discussed examples of dark patterns and their attributes, evidence of their prevalence online on businesses' websites or apps, consumers' vulnerability to them, as well as the tools and approaches available to consumer policy makers and authorities to identify and mitigate them. This report builds on the roundtable discussion, in particular by proposing a working definition of dark commercial patterns, further setting out evidence of their prevalence and harms, and identifying possible policy and enforcement responses to assist consumer policy makers and authorities in addressing them. It also documents possible approaches consumers and businesses may take to mitigate dark patterns.

More specifically, the report first discusses the nature of dark patterns and issues around their definition (Section 2), followed by their prevalence (Section 3), effects on consumer decision-making, detectability, and harms (Section 4), regulatory and enforcement measures (Section 5), and finally educational, technical and business initiatives and tools (Section 6). The report is also supported by annexes providing additional information.

In parallel to this report, the CCP is developing a report on consumer vulnerability in the digital age, which considers the impact on consumer vulnerability of several trends emerging from the digital transformation, including the increasing prevalence of dark patterns (OECD, forthcoming[10]).

2. What are dark commercial patterns?

Key points

- "Dark patterns" is an umbrella term referring to a wide variety of practices commonly found in online user interfaces that lead consumers to make choices that often are not in their best interests. Developing a universally accepted definition of dark patterns is a challenge, owing in part to the wide variety of practices referred to as such and different views on whether certain practices should be considered dark patterns. The OECD Committee on Consumer Policy proposes the following working definition intended to facilitate near-term discussion about such practices among regulators and policy makers across jurisdictions: *"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."*
- Many dark patterns influence consumers by exploiting cognitive and behavioural biases and heuristics, including default bias, the scarcity heuristic, social proof bias or framing effects. They generally fall in one of the following categories:
  - forced action, e.g. forcing the disclosure of more personal data than desired.
  - interface interference, e.g. visual prominence of options favourable to the business.
  - nagging, i.e. repeated requests to change a setting to benefit the business.
  - obstruction, e.g. making it hard to cancel a service.
  - sneaking, e.g. adding non-optional charges to a transaction at its final stage.
  - social proof, e.g. notifications of other consumers' purchasing activities.
  - urgency, e.g. countdown timer indicating the expiry of a deal.
- Dark patterns share one or more end-goals – for example getting consumers to purchase, purchase more of, or continue to purchase, a good or service that they would otherwise not purchase or purchase in lesser quantity; to spend more money on a purchase or time on a service than desired; or to give up more personal data than desired – with the ultimate purpose of increasing business revenue. In this way, they are inextricably linked to an underlying business model. Given competitive constraints, businesses may at times be incentivised to use them, particularly if there is no clear legal prohibition to doing so.
- Dark patterns may be of greater cause for concern than analogous practices in brick-and-mortar stores owing to a number of factors. These include businesses' increasing use of behavioural insights and leveraging of information asymmetries to hone user interface designs; consumers' online behaviours (such as a tendency to routinely ignore certain kinds of content); and the scale of consumers reachable online.

Nature of dark patterns

A user experience (UX) designer, Harry Brignull, coined the term "dark patterns" in 2010 to describe "tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something" (Brignull, n.d.[11]). The term, which is today widely used among computer and behavioural scientists working on user interface design, applies to a wide variety of online practices in user interfaces that steer, deceive, coerce, or manipulate consumers into making choices, including regarding purchases, their personal data or attention time, which may not be in their best interests. Prominent examples include user interfaces that trick a consumer into buying a product by falsely claiming it will sell out fast or by hiding important information. Dark patterns may also make it harder for consumers to make a choice in their interest, such as cancelling an unwanted service or selecting privacy-friendly settings.

While the term is relatively new, the concepts and mechanics it describes have been studied for some time in various fields. Consumer protection authorities have addressed online practices now characterised as dark patterns, such as drip pricing and subscription traps, through enforcement actions and policy initiatives for more than a decade (see Annex G for examples of enforcement actions). Behavioural scientists have long studied the role of cognitive and behavioural biases, such as default bias and loss aversion, in driving certain consumer purchasing decisions (e.g. Thaler and Sunstein (2008[12])). And marketers have long employed principles of behavioural economics to influence such decisions.

Similar terms and concepts have also been applied in other areas. "Sludge" describes the deliberate addition of frictions and hassles to make it harder to make choices in one's interests (Thaler, 2018[13]). "Evil" or "dark" nudges have been used to describe nudging that makes it easier to make choices against one's best interests (Petticrew et al., 2020[14]; ICPEN, 2019[15]; Thaler, 2015[16]). Legal scholars have also referred to "digital market manipulation" to describe similar phenomena to dark patterns (Hanson and Kysar, 1999[17]; Calo, 2014[18]).

Dark patterns vary across a range of dimensions and come in many different shapes and designs. They may employ different kinds of design-based elements (e.g. use of single or multiple screens; pop-up dialogue boxes or embedded text; variations in colouring and prominence of options, etc.) and text-based elements (e.g. use of emotive or aggressive language). They may appear in e-commerce websites, apps, cookie consent notices, search engines or online games, and can intervene at different stages of a transaction, such as the advertising, pre-purchase, payment or post-purchase stages. They may involve the collection and use of consumer data and/or the use of artificial intelligence technologies such as machine learning (CMA, 2021[19]; ACM, 2020[20]).

Nonetheless, all dark patterns rely on cognitive mechanisms to influence the consumer, possibly subliminally, and many exploit specific biases or heuristics.[3] These include default or status quo bias (a tendency to remain with the status quo or default option); the scarcity heuristic (a tendency to place higher value on scarce options); social proof bias (a tendency to make choices that conform with those of others); the anchoring effect (a tendency to base decisions around a particular reference point); the sunk-cost fallacy (a tendency to persist with a choice based on resources invested in it); and framing effects (a tendency to make different choices based on the same information depending on how it is presented).[4] Dark patterns have accordingly been characterised as strategies that seek to exploit what behavioural economist Daniel Kahneman has termed "System 1" thinking, involving automatic, intuitive decision-making with little cognitive effort, rather than the deliberative, conscious and effortful decision-making embodied in "System 2" thinking (Bösch et al., 2016[21]).

Taxonomies of dark patterns

With the increasingly wide variety of examples of practices qualified as dark patterns, much of the initial academic work on dark patterns has focused on collecting examples of them and categorising them through taxonomies (Conti and Sobiesk, 2010[22]; Bösch et al., 2016[21]; Gray et al., 2018[23]; Mathur et al., 2019[24]; Luguri and Strahilevitz, 2021[25]). The box below presents a non-exhaustive list of categories emerging from the literature, which relate mainly to dark patterns identified on websites and apps. Annex A provides visual examples of dark patterns for each of these categories.

Box 1. Categories of dark patterns

Forced action

Dark patterns involving forced action seek to force the consumer to do something in order to access a specific functionality (Gray et al., 2018[23]). Specifically, the consumer may be *forced to register* or be tricked into thinking it is necessary, or be *forced into disclosing* more personal information than desired, or, in the case of a free service, than required to use it fully. Another example is the extraction and usage of information about the consumer's contacts, possibly without the consumer's consent, in order to use a service (known as *friend spamming* or *social pyramid*).

Interface interference

Dark patterns involving interface interference aim to privilege specific actions from the consumer favourable to the online business through the framing of information (Gray et al., 2018[23]), and may exploit framing or anchoring effects or default bias. Examples include visually obscuring important information (*hidden information*); *preselection* of options favourable to the business by default; giving visual precedence to options favourable to the business, thus creating a *false hierarchy*; displaying a discounted price with reference to an original misleading or false higher price (*misleading reference pricing*); using intentional or obvious ambiguity with *trick questions* (e.g. double negatives); *disguising advertisements*; and manipulating the consumer toward a particular choice through emotive language or framing (known as *confirmshaming* or *toying with emotions*).

Nagging

Nagging dark patterns involve repeated requests to the consumer to do something favourable to the business, such as turn on notifications or location-tracking, and may thereby exploit the consumer's limited willpower or time.

Obstruction

Obstruction-related dark patterns aim to make a task flow or interaction more difficult than it may inherently need to be with the intent to dissuade an action (Gray et al., 2018[23]), and thus may exploit consumer inertia, or limited willpower or time. An example is making it easy to sign up to a service or opt in to privacy-intrusive settings but *hard to cancel* the service or *opt out* to more privacy-friendly settings. In a similar vein, *click fatigue* and *ease* refer to creating different lengths of click paths to different options in order to steer consumers to choose the "simple" path preferred by the business (Dapde, n.d.[26]; Forbrukerrådet, 2018[27]).[5] Other examples include making it hard or impossible to delete an account or consumer information (often termed *immortal accounts*) or to compare different offers and prices *(price comparison prevention*).

Sneaking

Sneaking dark patterns seek to hide, disguise, or delay the divulging of information relevant to the consumer's decision (Gray et al., 2018[23]), particularly regarding costs, and may exploit limited attention, default bias, the anchoring effect or sunk cost fallacy in consumers. Examples include adding new and potentially significant non-optional charges to the total price when a consumer is just about to complete a purchase (otherwise known as *drip pricing*); *sneaking an item* into a consumer's basket without consent e.g. via a checkbox on a prior page; or automatically renewing a purchase, including following a trial period, without the consumer's explicit consent (i.e. *hidden subscription / subscription trap*, also known as *forced continuity*). Providing a consumer with unsolicited goods or services is also more generally described as *inertia selling* or *negative option billing*.

Social proof

Dark patterns involving social proof attempt to trigger a decision based on observations of other consumers' behaviour, and can thus exploit social proof bias. Examples include *notifications about other consumers' activities* or *testimonials*[6] about their recent purchases. Activity notifications might not be truthful, e.g. where they falsely signal old purchases as if they were sold recently, and testimonials may be misleading or false.

Urgency

Dark patterns involving urgency impose a real or fake temporal or quantitative limit on a deal to pressure the consumer into making a purchase, thus exploiting the scarcity heuristic. Accordingly, such dark patterns may also be referred to as *scarcity cues* or *claims*. Examples include *low stock* and *high demand messages* or a *countdown timer* to indicate an expiring deal or discount.

It is unlikely that there will ever be a definitive and complete taxonomy of dark patterns, for several reasons. First, new forms of dark patterns are constantly emerging, with new technologies and new kinds of user interfaces, such that a taxonomy is unlikely to be future-proof (Rieger and Sinders, 2020[28]). Second, any taxonomy will reflect its authors' objectives (Luguri and Strahilevitz, 2021[25]) and the criteria for the inclusion of certain practices and exclusion of others. Some taxonomies seek to be comprehensive; for example, a 2022 European Commission (EC) study ("the 2022 EC study") aimed to classify all dark patterns according to two axes: the component of the choice architecture affected by the practice and the component of the consumer decision-making process that the practice targets to promote a behavioural change (EC, 2022[29]). Others focus on the kinds of dark patterns identifiable through a web-crawling process, which may lend themselves more to text- rather than design-based dark patterns (e.g. Mathur et al. (2019[24])). Some have been developed specifically with a certain policy area or activity in mind, such as privacy (Bösch et al., 2016[21]) or online games (Zagal, Björk and Lewis, 2013[30]).[7] In contrast, the United Kingdom (UK) Competition and Markets Authority's (CMA) taxonomy focuses more broadly on online choice architecture practices in general (both those harmful and beneficial to the consumer), classifying 21 such practices into three categories: choice structure, choice information and choice pressure (CMA, 2022[31]). Any taxonomy will also ultimately reflect the understanding or definition of dark patterns adopted (which vary significantly in the literature, see below). For example, in contrast to some earlier taxonomies, recent academic literature has considered the "infinite scroll" interface design allowing consumers to constantly scroll downwards to see new content (e.g. Cara (2019[32])) and the "autoplay" practice of automatically loading a video when the previous one ends (e.g. Bongard-Blanchy et al. (2021[33])) to be dark patterns.

The above caveats notwithstanding, Annex B provides an example of a consolidated, though non-exhaustive, taxonomy of the main dark patterns discussed in the literature to date, using the high-level categories discussed in the box above.

Novelty of dark patterns

Similar commercial practices to dark patterns have long been employed offline by brick-and-mortar stores to deceive and manipulate consumers into making sub-optimal decisions. Examples include falsely claiming a store is closing, or offering credit cards with low interest rates while indicating in fine print that the rate is set to rise significantly. The early days of the Internet also brought misleading online practices that have now been in use for some time, such as a pop-up window falsely telling the consumer about a free prize. What is then different about dark patterns in today's online world to warrant specific focus from consumer authorities and policy makers?

Several factors stand out. First, today's online businesses are much more aware of the opportunities afforded by behavioural insights to refine their marketing strategies (Narayanan et al., 2020[34]), including by exploiting key biases and heuristics affecting consumer behaviour online. Evidence indicates, for example, that consumers pay less attention to disclosures in an online environment (OECD, 2018[5]; OECD, forthcoming[35]), process information less well when shopping and consuming information online and more frequently default to simple rules of thumb when faced with information overload (Firth et al., 2019[36]; Jerath, Ma and Park, 2014[37]; Mangen, Walgermo and Brønnick, 2013[38]). Moreover, research shows that consumers interact with digital interfaces in a task-focused way, leading them to routinely ignore certain kinds of content (Willis, 2020[39]; OECD, forthcoming[35]), and underestimate manipulation and deception in online more than offline contexts (Moran, 2020[40]). Indeed, as discussed in Section 4, often consumers are unaware of the harms of dark patterns. A growing body of evidence also shows that consumers have greater difficulty processing information on mobile devices (see e.g. Amazeen (2021[41]) and more broadly Section 4 discussing evidence of dark patterns' effects on mobile devices).

Second, in contrast to face-to-face transactions, transactions between consumers and online businesses are mediated through an interactive and connected device, such as a computer or mobile phone (Calo, 2014[18]). That allows online businesses to collect data on how consumers interact with the business through the device and optimise their commercial practices accordingly. In particular, online businesses can repeatedly conduct randomised experiments, known as A/B testing, involving serving variants of web pages to two or more randomly selected subsets of consumers, so as to continuously hone the design of websites and apps based on which configurations maximise the outcomes they are seeking from consumers (Narayanan et al., 2020[34]). Machine learning can help optimise this process (Kinnaird, 2020[42]). Accordingly, very granular aspects of the choice architecture in a user interface, such as the position of a "Buy" button, the colour of an information banner and a default payment method, can be optimised to maximise conversion rates (i.e. the proportion of consumers who go on to make a purchase after visiting an e-commerce website), all the while giving consumers an illusion of control (CMA, 2021[19]; Willis, 2020[39]). As a result, the effect sizes of dark patterns on consumer decision-making, as further detailed in Annex D, can be substantially larger than those of manipulative tactics employed in brick-and-mortar stores (Luguri and Strahilevitz, 2021[25]). Indeed it is the information asymmetry resulting from increasingly transparent online consumer behaviour compared to largely opaque business processes that is considered to be at the core of consumer manipulation through dark patterns (Kemp, 2020[43]; Forbrukerrådet, 2018[27]). Furthermore, human-operated A/B testing experiments may gradually be replaced with algorithmic marketing, involving the autonomous experimentation and adaptation of marketing techniques with reference to a business objective. Lack of human involvement may mean that such tests lack appropriate oversight and could inadvertently lead to more detriment (Willis, 2020[39]; CMA, 2021[19]; ACM, 2020[44]).

Finally, the scale of consumers that can be reached through a single business' dark patterns at low cost, in particular a major online platform, is significantly higher than it is for analogous practices offline, such that the potential for consumer detriment is markedly greater (OECD, 2021[9]).

Origins of dark patterns and incentives for their use

The ultimate purpose of dark patterns is to increase business revenue, whether in terms of sales or proceeds of advertising. They do so in multiple ways, including by getting consumers to purchase, purchase more of, or continue to purchase, a good or service which they would otherwise not purchase or purchase in lesser quantity; to spend more money on a purchase or time on a service than desired; or to give up more personal data than desired. In this way, dark patterns reflect the downstream marketing impacts of a broader corporate strategy and are thus inextricably linked to an underlying business model. For example, dark patterns that deceive consumers into giving up more data than desired (e.g. through hidden privacy-intrusive settings turned on by default) or manipulate them into spending more time on a website (e.g. through addictive interface design) might support a business model involving capturing consumer attention and collecting consumer data for advertising, e.g. of an online platform. Dark patterns that force registration for a subscription trial, automatically renew an original purchase without the consumer's explicit consent or make it hard to cancel a subscription might support a business model involving rapid expansion of an online user base, e.g. of an online subscription service.

Hence dark patterns do not come about by chance; indeed designers are often incentivised to develop user interfaces that perform well in terms of metrics relevant to the business model (e.g. conversion rates, sales, time spent on website, data collected). A/B testing helps to determine which user interfaces perform best according to those metrics, and often those employing dark patterns perform better (Narayanan et al., 2020[34]; Brignull, 2021[45]). Nonetheless, there are many examples of successful online business models relying on user interfaces that do not incorporate dark patterns. Furthermore, designers may often bear no malicious intent or be unaware that their interfaces incorporate dark patterns (Willis, 2020[39]). Indeed, research shows designers often feel motivated to act ethically, but may be restricted in their ability to do so due to commercial pressures and may have limited understanding of their capacity to affect consumer decisions, such as regarding privacy (Beattie, Lacey and Caudwell, 2020[46]). Moreover, where interface design is automated through algorithmic optimisation, there may not be a human designer actively implementing a dark pattern (Willis, 2020[39]).

The use of certain dark patterns, such as scarcity cues or activity notifications, is sometimes facilitated by third-party entities that provide the ability to create and implement dark patterns on e-commerce websites, often through plugins (Mathur et al., 2019[24]). Furthermore, in response to the introduction of the European Union's (EU) General Data Protection Regulation 2016/679 (GDPR), third-party consent management platforms (CMPs) emerged to facilitate the handling of consent to tracking on EU websites via consent notices, which have also been found to contain dark patterns in their user interface designs (see Section 3 for more details). In some circumstances, false testimonials may potentially reflect criminal activity in some jurisdictions.

Market forces may also pressure online businesses to use dark patterns, particularly where they are not clearly prohibited, to remain competitive. Research has demonstrated that, in the presence of consumer biases in competitive markets, firms may have greater incentives to engage in behavioural exploitation such as drip pricing (Gabaix and Laibson, 2006[47]). The increasingly barrier-free environment of online markets may further contribute to businesses engaging in a "race to the bottom" through dark patterns, e.g. that capture consumer consent and/or agreement, while forgoing legal obligations (Leiser, 2020[48]). As noted by the Stigler Committee on Digital Platforms ("the Stigler Committee"), businesses wishing to avoid dark patterns may struggle to compete where consumers are either unable to detect or have become accustomed to the dark patterns in market use and hence do not switch to businesses that do not use dark patterns (Stigler Committee, 2019[49]).

Even if certain aggressive dark patterns may drive some consumers away, the increased revenue from the bulk of consumers on whom they are effective may still incentivise their use, and over time businesses may seek to determine the profit-maximising usage of dark patterns (Egberts, 2021[50]). For example, in the United States (US), after a ticket reseller found through an experiment in 2015 that customers spent over 20 percent more on tickets when mandatory fees were hidden until the end of the transaction versus disclosed at the start, it resumed its practice of hiding mandatory fees in order to remain competitive (Sarinsky, 2021[51]). Nonetheless, to the extent consumers recognise and reject dark patterns, some commentators have suggested that any short-term gains an online business gets from dark patterns are likely to be lost in the long term (Brownlee, 2016[52]).

Challenges to developing an international definition of dark patterns

While there is broad consensus on examples of dark patterns, a universally accepted definition is yet to emerge. Definitions developed in the academic and policy literature to date vary in terms of characteristics of the user interface of the website or app, mechanisms of effects on users, the role of user interface designers and the outcomes for the online business or the consumer (Mathur, Kshirsagar and Mayer, 2021[53]). Common notions reflected in definitions include deception, manipulation, coercion, or exploitation in the design of user interfaces that lead consumers to make decisions that may not reflect or engage their true preferences, intent, consent, autonomy or best interests. These notions are also reflected in recent legislative text, as shown in the box below.

Box 2. Examples of definitions of dark patterns in existing or proposed legislation

California Privacy Rights Act (CPRA)

The CPRA, which was passed in 2020, is understood to be the first legislation to provide a definition of dark patterns, as follows: *"a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation"* (CPRA/ Cal. Civ. Code § 1798.140(l)).

EU Digital Services Act (DSA) and Digital Markets Act (DMA)

The DSA, EU legislation adopted in 2022 that will place new obligations on online platforms and intermediaries, defines dark patterns as follows in its preamble: *"Dark patterns on online interfaces of online platforms are practices that materially distort or impair, either purposefully or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions."* (Recital 67) (EP, 2022[54]). A prohibition on online platforms designing, organising or operating online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of recipients of their service to make free and informed decisions applies in Article 25. Similarly, under the DMA, EU legislation adopted in 2022 placing new obligations on very large online platforms ("gatekeepers"), a prohibition also applies on gatekeepers offering choices to the end-user in a non-neutral manner, or subverting end users' or business users' autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface or a part thereof (Article 13) (EP, 2022[55]).

US Deceptive Experiences To Online Users Reduction (DETOUR) Act

The DETOUR Act, the first federal legislation proposed in the US aiming to prohibit dark patterns on online platforms (which was first tabled in 2019 but had not passed at the time of writing), does not define dark patterns. However it would make unlawful for any large online platform *"to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data"*.[8]

Some definitions in the literature may appear too narrow to cover all dark patterns. Specifically, according to Mathur, Mayer and Kshirsagar (2021[53]), several definitions indicate that dark patterns:

- are designed with the *intent* to influence consumer choice. However, as discussed above, malicious intent may not always drive the development of dark patterns; indeed draft regulations released in 2022 by the California Privacy Protection Agency (CPPA) for the CPRA, which were subject to public comment at the time of writing, sought to specify that practices can be dark patterns "regardless of business intent".[9]
- *benefit* a business or *harm* the user. However, as discussed in Section 4, the harms of dark patterns may often be difficult or impossible to identify, such that a definitional requirement of harm or benefit could risk inadvertently leaving certain commonly recognised dark patterns outside the scope of the definition.

- are *deceptive*. But some dark patterns do not necessarily deceive consumers. For example, Mathur, Mayer and Kshirsagar (2021[53]) assert confirmshaming is not deceptive as it is often entirely transparent, and Hung (2021[56]) asserts that nagging is neither deceptive nor necessarily manipulative in that it relies on persistent repetition to wear the consumer down to desired action. As outlined by Susser, Roessler and Nissenbaum (2019[57]), persuasion, deception, manipulation and coercion can be considered related but subtly different forms of influence (and such distinctions may have implications for enforcement - see Section 5 for details).

Furthermore, while most dark patterns identified in the literature appear in online user interfaces, this is not explicitly the case for some. For example, some dark patterns may be considered to have more to do with frictions in processes rather than the user interface specifically (e.g. making a service hard to cancel by requiring a phone call). In this regard, the CMA and the Netherlands Authority for Consumers & Markets (ACM) use the broader term of online choice architecture, which for the ACM relates to both the user interface and the customer journey online (ACM, 2020[20]). And some dark patterns, while of a digital nature, may operate without an Internet connection - e.g. in children's apps (Radesky et al., 2022[58]) or in ATMs.[10]

Notwithstanding variations in definitions, Mathur, Kshirsagar and Mayer (2021[53]) find that what binds together the practices qualified as dark patterns in the literature is that they *modify the choice architecture presented to the consumer*. This is done either by *modifying the set of choices available* to the consumer (by applying unequal burdens on available choices, eliminating choices that should be available or treating some consumers differently than others) or by *manipulating the information flow* to the consumer (by providing false information or obscuring or delaying relevant information).

Still, some commentators have provided examples of practices that might be considered dark patterns in some but not all contexts. For example, even though recommendations based on purchase history or the infinite scroll and autoplay designs might lead some consumers to spend more money or time than intended on an online platform, other consumers may prefer to have such features if they allow them to easily discover further products or content of interest (Alavi, 2020[59]; Otto, 2020[60]). Hurwitz (2020[61]) notes that use of visual prominence to promote one purchase option over another can sometimes reflect the preferences of the majority of consumers, inviting questions about whether the practice may be considered a dark pattern in such circumstances. Other commentators have noted that scarcity or popularity claims, if truthful, may provide useful information about the level of demand for offerings and hence should not be considered dark patterns (even though some consumers may assign undue weight to the product's popularity) (Luguri and Strahilevitz, 2021[25]; Stigler Committee, 2019[49]).[11]

Further complicating the delineation of dark patterns is the difficulty in demarcating them from legitimate or acceptable persuasive marketing practices. The preamble to the DSA specifies that legitimate commercial practices that comply with EU law should not be considered dark patterns (EP, 2022[54]).[12] Luguri and Strahilevitz (2021[25]) offer the distinction that most dark patterns aim to manipulate the consumer into a choice inconsistent with their preferences, whereas marketing efforts seek to alter those preferences. Yet some marketing techniques that have long existed offline and online and have been largely normalised by consumers and tolerated by consumer authorities might also play on cognitive biases and manipulate consumers to some degree. For example, commonly used psychological pricing strategies, such as reducing the left digit of a price by 1 and increasing the others to 9 (e.g. "USD 4.99" instead of "USD 5.00"), have been shown to incentivise consumers to pay more than they otherwise would in ways that may be unknown to the consumer (Bizer and Schindler, 2005[62]; Repetto and Solís, 2020[63]). The choice architecture in supermarkets is often designed to exploit consumer biases, e.g. by placing products with the highest margin at eye level or placing fruit and vegetables at the entrance so consumers feel less guilty about subsequently selecting unhealthy food. And similar to confirmshaming, advertising to buy life insurance might typically seek to evoke emotions of guilt and shame of not doing so (Sunstein, 2016[64]). In this regard, Sunstein (2016[64]) asserts that there are different shades of manipulative practices, some of which may be more acceptable than others – such as nudging a consumer into a default pension allocation or more sustainable consumption. In a similar vein, Willis (2020[39]) notes a lack of societal consensus on what constitutes acceptable non-deceptive manipulation and thus prefers to limit her analysis to clearly deceptive dark patterns, and Jarovsky (2022[65]) considers a practice's manipulative character, without a malicious element, would not alone suffice to classify it as a dark pattern.

To address these difficulties, some researchers have suggested that specific thresholds could determine whether a practice could be considered a dark pattern. For example, Mathur, Mayer and Kshirsagar (2021[53]) suggest that a range of absolute and relative thresholds, based on different normative perspectives, could be applied to assess whether a practice should be considered a dark pattern. In some cases, such a threshold might be the bar of deceptiveness as defined by law. In other cases empirical metrics might be needed to assess the effect of the practice relative to an appropriate "baseline" user interface. In that regard, Luguri and Strahilevitz (2021[25]) propose that if the consumer uptake rate of an offering associated with a specific practice in a user interface is more than doubled in comparison to an alternative "neutral" user interface, the practice could be considered a dark pattern as the uptake could be more likely than not attributable to it. However, such approaches could also lead to further questions as to what constitutes an appropriate threshold. For example, some commentators have raised concerns that the "average consumer" benchmark in the EU Unfair Commercial Practices Directive 2005/29/EC (UCPD) used to determine whether a commercial practice is unfair does not adequately capture practices disproportionately harming consumers who, in some circumstances, would not meet the "average" standard and could be more vulnerable to such practices (see e.g. Howells, Twigg-Flesner and Wilhelmsson (2017[66]) and more generally OECD (forthcoming[10])). There may also be uncertainty as to what constitutes a "neutral" or "baseline" user interface; indeed, some researchers consider that all design influences consumers in some way and as such there is no neutral way to present choices (Schneider, Weinmann and Brocke, 2018[68]; Acquisti et al., 2017[69]; Hung, 2021[56]).

An OECD working definition of dark commercial patterns

Taking into account the above challenges and caveats, the OECD CCP has developed a working definition of dark commercial patterns to facilitate near-term discussion about such practices among regulators and policy makers across jurisdictions. Key principles guiding its development were that it be sufficiently broad to capture the range of practices to which the term has been commonly applied in the literature and that it assist in distinguishing dark commercial patterns from persuasive marketing practices in general. Building on existing definitions in legislative texts outlined in Box 2, it seeks to clarify that at the core of dark patterns is their objectionable effect on consumers' ability to make free and informed choices, with the likelihood of entailing consumer detriment. It reads as follows:

> *"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."*

The full definition appropriate in a particular setting may depend on whether it is intended for policy analysis or regulatory application, and on the larger legal context in which it is used. It could also evolve over time, depending on technological and regulatory developments. The possible forms of consumer detriment resulting from dark patterns are further discussed in Section 4.

3. Prevalence of dark commercial patterns

Key points

- Dark patterns are common on e-commerce websites and apps, including those of major online platforms, cookie consent notices, search engines and games. However, the frequency of dark patterns identified by researchers varies widely, owing to a range of factors including the research methodology applied.
- Many websites and apps feature more than one dark pattern, particularly popular ones.
- Their high prevalence on cookie consent notices may, in some jurisdictions, indicate high rates of violation of data protection laws.
- The relatively more frequent types of dark patterns identified on e-commerce websites and apps are countdown timers, low-stock messages, activity notifications, misleading testimonials, false hierarchy of options, pre-selection of specific options, forced registration or disclosure of personal data, disguised ads, nagging and making it hard to cancel/opt out. Less common are hidden costs, sneaking items into the basket, making it difficult to compare prices or delete an account, trick questions or friend spamming.
- Major online platforms and a significant proportion of cookie consent notices often use dark patterns involving "confirmshaming", making it hard to cancel or opt out, preselecting or creating a false hierarchy of options and hiding essential information, particularly with a view to steering the consumer to more privacy-intrusive settings.
- Third-party entities are often used to facilitate the implementation on e-commerce websites of activity notifications, which may be false or misleading.

Evidence of prevalence of dark patterns

Earlier research has documented the prevalence of specific dark patterns without necessarily using the "dark pattern" term. For example, several studies or sweeps have documented the prevalence online of subscription traps or drip pricing (ECC Sweden, 2017[70]; Citizens Advice, 2016[71]; EC, 2016[72]).[13] However, research focusing on the prevalence of a range of different dark patterns on e-commerce websites, apps, major online platforms, cookie consent notices and search engines has only recently emerged. An increasing number of enforcement actions in jurisdictions is also shedding light on dark patterns' prevalence (see Annex G for an overview).

The overall frequency of dark patterns detected on e-commerce websites and apps varies significantly in existing research. For example, according to research from:

- Mathur et al. (2019[24]), 11.1% of around 11 000 popular e-commerce websites examined featured dark patterns.
- a sweep conducted by the International Consumer Protection Enforcement Network (ICPEN) in 2019, 24 % of 1754 e-commerce websites/apps investigated featured "dark nudges" (ICPEN, 2019[15]).
- a sweep conducted in 2021 by the Chilean consumer protection authority, SERNAC, 64% of 103 Chilean e-commerce websites examined featured at least one dark pattern (SERNAC, 2021[72]).

- Radesky et al. (2022[58]), 80% of popular children's apps contained at least one manipulative design feature.
- Di Geronimo et al. (2020[73]), 95% of a sample of 240 popular apps contained at least one dark pattern.
- The 2022 EC study, 97% of 75 popular e-commerce websites and apps in the EU contained at least one dark pattern (EC, 2022[29]).
- Gunawan et al. (2021[74]), all 105 of the most popular online services in the Google Play Store that featured both an app and website format contained at least one dark pattern.
- Moser, Schoenebeck and Resnick (2019[75]), all 200 of the most popular online retailers in the US contained at least four instances of "impulse buying features".

Several of such studies or sweeps identified considerably more than one dark pattern on many websites and apps. For example, Di Geronimo et al. (2020[73]), found 49% of apps sampled included seven or more dark patterns in their user interfaces; Gunawan et al. (2021[74]) found the majority of online services had seven or more types of dark pattern; and the 2022 EC study found each website/app reviewed to have multiple dark patterns (EC, 2022[29]). Evidence from both Mathur et al. (2019[24]) and Gunawan et al. (2021[74]) also shows that popular e-commerce websites and apps tend to feature more dark patterns.

Variations highlighted above in the frequency of dark patterns detected may depend on several factors, including:

- *Medium or modality.* Gunawan et al. (2021[74]), for example, found dark patterns to be more prevalent in the app version of online services than the website version (though the 2022 EC study found similar prevalence levels for mobile apps and websites (EC, 2022[29])).
- *Type of websites/apps sampled.* The 2022 EC study, for example, found countdown timers and limited time messages to be among the more prevalent dark patterns on online goods retailers and marketplaces, while nagging was more common in health and fitness websites/apps (EC, 2022[29]).
- *Identification method.* For example, Mathur et al. (2019[24]) used an automatic web crawler that could only explore the product pages and cart pages of websites and only analyse textual information (rather than e.g. style or colour). More broadly, Stavrakakis et al. (2021[76]) submit that several dark patterns may not be detectable at all via a web crawler. In contrast, Di Geronimo et al. (2020[73]) employed human researchers to identify dark patterns by performing a range of different actions on apps, such as creating an account and logging out, closing and reopening the app and continuing shopping until checkout.
- *Types of dark patterns considered.* For example, Gunawan et al. (2021[74]) included the "gamification" dark pattern in their list of dark patterns to identify, while Di Geronimo et al. (2020[73]) did not.
- *Dark pattern definition.* For example, many of the "impulse buying features" identified by Moser, Schoenebeck and Resnick (2019[75]) on US e-commerce websites would not necessarily qualify as dark patterns (e.g. member/rewards program discounts). Moreover, Mathur et al. (2019[24]) found that a large proportion of the most frequent dark patterns they encountered – activity messages, countdown timers and low-stock messages – did not involve false information, and hence might not be considered dark patterns by some commentators (see Section 2).

- *Jurisdiction.* Variation in dark pattern frequency detected in studies carried out in different jurisdictions may also reflect differences in permitted practices.

The literature on the prevalence of dark patterns in cookie consent notices paints a somewhat more uniform picture. For example, Utz et al. (2019[77]) identified interface designs to steer website visitors towards accepting privacy-unfriendly options, such as preselected checkboxes and variations in visual prominence of options, on 57.4% of cookie consent notices on the most popular websites in the EU. Matte, Bielova and Santos (2020[78]) similarly identified use of preselection to steer consumers to privacy-unfriendly settings on 46.5% of cookie consent notices on popular European websites. Nouwens et al. (2020[79]) found that 56.2% of consent notices on the most popular UK websites used pre-ticked options and 50.1% did not have a "reject all" button. Soe et al. (2020[80]) found that 95% of consent notices on news outlets in Scandinavia, the UK and US did not provide a way to deny consent with one click (though all provided a one click "accept" button). Such literature has broadly concluded that rates of violation of data protection laws applicable in relevant jurisdictions as a result of dark patterns are likely to be high. Other research also determined there were high rates of breach of the EU GDPR in European and German cookie consent notices respectively owing to dark patterns (noyb, 2021[81]; VZBV, 2021[82]).

Targeted research regarding major online platforms conducted by some consumer authorities (the Australian Competition and Consumer Commission (ACCC) and the CMA), and the Norwegian Consumer Council (Forbrukerrådet) as well as a spate of recent enforcement cases have also shown that such platforms often use several specific kinds of dark patterns, such as *preselection, hidden information, false hierarchy, confirmshaming* and *hard to cancel*, particularly with a view to steering consumers to privacy-intrusive settings (Forbrukerrådet, 2018[27]; Forbrukerrådet, 2018[83]; ACCC, 2019[84]; CMA, 2020[85]; Forbrukerrådet, 2021[86]).

Furthermore, other studies have identified dark patterns in search engines and browsers (hard to cancel, preselection, nagging and false hierarchy) (ACCC, 2021[88]) and in games, particularly in the design of loot boxes (Zagal, Björk and Lewis, 2013[30]; Goodstein, 2021[89]; Forbrukerrådet, 2022[90]) (i.e. features containing randomised items that players access through gameplay or purchase with in-game items, virtual currency or real-world money (UK DCMS, 2020[91])).

On the whole, notwithstanding variations in the frequency of dark patterns identified in available evidence, these findings confirm that dark patterns are far from a niche practice. Though it bears recalling, as discussed in Section 2, that some businesses employing dark patterns may not have specifically intended to deceive or manipulate consumers, and that there is a lack of consensus on whether certain practices constitute dark patterns.

While drawing definitive conclusions on the relative prevalence of different kinds of dark patterns is difficult in light of the factors highlighted above, available evidence reviewed for this report suggests that the relatively more frequent dark patterns on e-commerce websites and apps in general are *false hierarchy*, *pre-selection, hidden information*, *disguised ads, nagging*, *hard to cancel/opt out, forced registration, forced disclosure,* urgency-related dark patterns (e.g. *countdown timers* and *low-stock messages*) and social proof-related dark patterns (*activity notifications* and *misleading testimonials*). *Pre-selection, false hierarchy* and *hard to cancel* dark patterns are also more prevalent on cookie consent notices. In contrast, the evidence reviewed for this report suggests that dark patterns involving sneaking (e.g. hidden costs, bait and switch, sneak into basket, hidden subscriptions – except in apps (ACCC, 2021[92])) and the intermediate currency, price comparison prevention, immortal accounts, gamification, friend spamming/social pyramid and trick questions dark patterns are relatively less prevalent on e-commerce websites and apps in general. Moreover, design-based dark patterns appear to be no less common than text-based ones.

See Annex C for an overview of selected evidence of the prevalence of dark patterns in various areas.

Evidence of prevalence of third-party entities facilitating dark patterns

In their web crawl, Mathur et al. (2019[24]) identified 22 third-party entities facilitating the implementation of dark patterns in 1 066 of the approximately 11 000 shopping websites sampled, of which two openly advertised practices enabling deceptive messages. Use of third-party entities was in particular frequent in relation to social proof-related *activity notifications*. Entities could be classified into two groups, providing either exclusively activity notifications integration or a range of marketing services often enabling other dark patterns, such as scarcity cues. Many of the third-parties' advertised practices appeared to be manipulative by making clear reference to exploitation of cognitive biases "[p]lay upon [customers'] fear of missing out by showing shoppers which products are creating a buzz on your website". Some offered the option of tailoring activity notifications to consumers' preferences and backgrounds, and some openly advertised the ability to create fake social proof messages.

4. Effects on consumer decision-making, detectability and harms to consumers

Key points

- Dark patterns can influence consumer decision-making substantially. They seem more effective on mobile devices and when combined or layered on multiple screens of a website or app.
- But individual dark patterns differ in their effectiveness. For example, hidden information appears substantially more effective than scarcity cues. Seemingly "mild" dark patterns (such as preselecting options or framing them differently) may be as or more effective than aggressive ones (such as nagging and toying with emotions).
- The effectiveness of some dark patterns may be driven by their subtlety and difficulty of detecting them, which may in turn relate to a consumer's prior experience with the dark pattern, intrinsic difficulty in spotting it or its general pervasiveness.
- By hindering consumers' ability to make free and informed choices, dark patterns impair consumer autonomy. Some dark patterns may also cause personal consumer detriment in terms of financial loss (e.g. drip pricing and subscription traps), privacy harms, psychological detriment (relating to expended energy or attention and emotional distress) as well as time loss.
- Dark patterns may furthermore cause structural consumer detriment by affecting consumers collectively, through impacts on competition or trust in online businesses.
- Some consumers are likely to be disproportionately affected by dark patterns, such as less educated consumers or children. While there is no robust evidence yet to suggest that personalised dark patterns triggering personal vulnerabilities are commonly used, this is likely to change with businesses' increasing data collection combined with machine learning and other AI techniques.
- Concrete evidence of consumer detriment from dark patterns is lacking in many cases, however, meaning further research is needed to appropriately guide policy and enforcement responses.

While many commentators have pointed to the harmful impacts of dark patterns on consumers, the empirical evidence to support such claims is still emerging. Moreover, as raised in Section 2, it is not clear that all dark patterns are equally problematic for consumers; researchers have pointed to the varying degrees of "darkness" in dark patterns (Gray et al., 2018[23]; Hurwitz, 2020[61]). Yet, an understanding of the effects on consumer decision-making of different dark patterns and the resulting harms is vital to guide consumer policy makers and enforcers in prioritising which dark patterns to address.

Evidence of the influence of dark patterns on consumer decision-making and their detectability

Some studies have assessed the effects of specific dark patterns on consumer decision-making, or of the mechanisms they involve, without necessarily using the "dark pattern" terminology. These include hidden subscriptions (EC, 2016[72]; ECC Sweden, 2017[70]), disguised ads (EC, 2018[93]), pre-selection,[14] or hidden charges/drip pricing (see Annex E for further details on the latter). In a review of evidence regarding effects of online choice architecture practices on consumer behaviour, the CMA found that there is substantial evidence of the power of default settings (which may relate to e.g. the preselection or hidden subscription dark patterns), drip pricing and reference pricing (CMA, 2022[31]).

While the first wave of scholarship on dark patterns has focused on taxonomies, and a second on prevalence, a third wave has begun to empirically assess the effects of several different dark patterns on consumer decision-making, sometimes in comparison with each other or in combination, typically with behavioural experiments and consumer surveys. That literature shows that a range of dark patterns, such as *hidden information, hard to cancel/opt out, preselection, false hierarchy, social proof/activity messages* and *trick questions,* can influence consumer decision-making substantially (see e.g. Luguri and Strahilevitz (2021[25]) and the 2022 EC study (EC, 2022[29])). *Pre-selection*, *false hierarchy*, and *hard to cancel/* dark patterns have also been found particularly effective in cookie consent notices (Machuletz and Böhme, 2019[94]; Utz et al., 2019[78]; Graßl et al., 2021[95]).

Luguri and Strahilevitz (2021[25]) have also identified the cumulative effectiveness of combined dark patterns, showing for example that hidden information combined with an obstruction dark pattern influence consumer decision-making more than either dark pattern alone. This could result either from interactions between the dark patterns or the increased chance that at least one dark pattern will be effective. Such evidence provides further context to findings in Section 3 that major online platforms, cookie consent notices and a majority of apps tend to feature multiple dark patterns.

Furthermore, evidence points to the greater effectiveness of dark patterns on mobile devices or smaller screens, where information is less prominent (Utz et al., 2019[78]; Strahilevitz, 2021[96]). Supporting such findings, other research shows greater cognitive effort is required to distinguish news from covert advertising on mobile screens (Amazeen, 2021[41]).

However, individual dark patterns differ in their effectiveness in influencing consumer choice. For example, Luguri and Strahilevitz (2021[25]) and the 2022 EC study (EC, 2022[29]) found *hidden information* was more effective in influencing consumers than certain other dark patterns such as social proof, scarcity cues and confirmshaming/toying with emotions. Other empirical evidence indicates mixed effectiveness of scarcity cues relative to social proof. Specifically, Sin et al. (2022[96]), Teubner and Graul (2020[98]), and Drossos, Zacharioudakis and Dionysiou (2019[97]) found both social proof and scarcity cues to boost conversion rates/purchase intentions or impulse buying. But Luguri and Strahilevitz (2021[25]), a 2020 EC study on marketing practices in online travel booking ("the 2020 EC study") (EC, 2020[101]) and Jeong and Kwon (2012[99]) found social proof effective but scarcity cues ineffective, and Keizer (2017[101]) found both ineffective, though social proof less so. That social proof may be more effective than scarcity cues is supported by evidence reviews, with Sin et al. (2022[96]) identifying a large body of research affirming the effectiveness social proof in general (reviews, ratings, and recommendations) and Ahmetoglu, Furnham and Fagan (2014[102]) finding mixed evidence in the literature of time-limited offers. Empirical evidence regarding confirmshaming also appears mixed; for example, Luguri and Strahilevitz (2021[25]) found it effective but the 2022 EC study (EC, 2022[29]) ineffective.

Moreover, Luguri and Strahilevitz (2021[25]) showed that seemingly "mild" or subtle dark patterns, such as a preselected "Accept and continue (recommended)" button (preselection and false hierarchy) combined with an "Other options" button (making it harder to decline than accept) can be as effective as more aggressive ones (such as nagging and toying with emotions) and spark little backlash from consumers. This suggests that dark patterns' *effectiveness* in influencing consumers may depend in part on their *detectability* or *subtlety*. Recent empirical literature focusing on perceptions and detectability of dark patterns tends to support this view. In particular, evidence indicates that many consumers are blind to dark patterns (Di Geronimo et al., 2020[73]; Maier and Harr, 2020[103]); that consumers who more easily recognise manipulative designs consider themselves slightly less likely to be influenced (Bongard-Blanchy et al., 2021[33]); that consumers accept subtle dark patterns as part of the normal digital experience (EC, 2022[29]); and that the misleading character of a dark pattern is less noticed when its design is more appealing and thus considered more trustworthy (Bhoot, Shinde and Mishra, 2020[104]).

Evidence from Bhoot, Shinde and Mishra (2020[104]), Bongard-Blanchy et al. (2021[33]) and Di Geronimo et al. (2020[73]) taken together suggests confirmshaming, scarcity cues, forced continuity and bait and switch are among the most detectable dark patterns, whereas *hard to cancel*, *forced disclosure*, *preselection, hidden information* and *trick questions* are among the *least detectable*. Several factors may determine detectability. Bhoot, Shinde and Mishra (2020[104]) found it linked to consumers' prior experience with the dark pattern. In support of this, Luguri and Strahilevitz (2021[25]) and the 2022 EC study (EC, 2022[29]) advance that countdown timers and confirmshaming, respectively, may be ineffective as they have become commonplace. Bongard-Blanchy et al. (2021[33]) suggest that some dark patterns, such as hidden information, are intrinsically more difficult to spot, and that pervasiveness might explain difficulties in detecting others, such as preselection and forced disclosure. Indeed research by Graßl et al. (2021[94]) suggests that consumers may have become conditioned to selecting the privacy-unfriendly choice in cookie consent notices such that they do not notice that dark patterns are at play. Similarly, in the case of nagging, knowing that eventually consumers may need to agree to push notifications to use a particular service, over time they may simply choose to authorise them immediately (Strahilevitz, 2021[96]).[15]

However, evidence also indicates consumers may be influenced even when they are aware that choice architecture is being used against them (Loewenstein et al., 2015[105]; Bongard-Blanchy et al., 2021[33])), such that awareness may not always be sufficient to protect consumers (CMA, 2022[31]). Accordingly, detectability may be a less significant criterion by which to prioritise policy and enforcement responses to dark patterns than their prevalence, effectiveness and detriment (see Section 5 for more details on using evidence to prioritise policy and enforcement efforts).

Finally, research shows that certain "bright patterns", i.e. user interface designs that aim to steer consumers toward consumer-friendly options, can be effective. These include choice architectures that provide consumers with more granular consent choices (Nouwens et al., 2020[80]) or that make privacy-friendly options easier to select than privacy-intrusive options, e.g. through preselected defaults or aesthetic framing (Graßl et al., 2021[94]; SERNAC, 2022[106]).

Annex D provides an overview of evidence identified concerning the comparative effects of dark patterns on consumer decision-making and their detectability.

Harms of dark patterns to consumers

While some research has explored the effects of dark patterns on consumer decision-making, less has been done on assessing the ultimate harms they cause consumers. As Mathur, Kshirsagar and Mayer (2021[53]) point out, the dark patterns literature has largely focused on the descriptive aspects of dark patterns. They submit that underlying such descriptions is a set of nascent normative concerns attempting to explain why dark patterns should be of concern: individual and collective welfare, regulatory objectives, and individual autonomy. These normative perspectives mirror the conceptual distinctions made between harms to autonomy and harms to welfare by some researchers (Susser, Roessler and Nissenbaum, 2019[108]; Zarsky, 2019[109]) and between personal and structural consumer detriment (understood as consumer welfare losses) in the OECD Consumer Policy Toolkit (OECD, 2010[6]). They serve as a starting point for understanding the various harms that dark patterns may cause. Accordingly, the following sub-sections explore such harms in terms of impacts on consumer autonomy and personal and structural consumer detriment. The relationship between dark patterns and regulatory frameworks is explored in Section 5.

Harms to consumer autonomy

Personal autonomy has been defined as the capacity to make one's own choices, by having the competency to do so and being able to authentically endorse the reasons for them (Susser, Roessler and Nissenbaum, 2019[57]). Hence dark patterns can be considered to compromise consumers' personal autonomy to the extent that they lead consumers to make choices they may not otherwise have made, deny consumer choice,[16] obscure available choices, or burden the exercise of choice (Mathur, Kshirsagar and Mayer, 2021[53]). This is especially true considering dark patterns may often provide the illusion of, rather than actual, control to consumers (Forbrukerrådet, 2018[27]; Willis, 2020[39]). Dark patterns that explicitly affect consumer autonomy include those relating to forced action or obstruction; those relating to interface interference or sneaking have a more covert influence on consumer autonomy.

That the subversion or impairment of consumer autonomy, decision-making or choice are defining characteristics of dark patterns is reflected in the proposed working definition set out in Section 2. As the definition also suggests, this can in turn result in different forms of personal and structural detriment highlighted below, to the extent that many can be traced back to a hindrance in ability to make free and informed choices. Reductions in autonomy through online manipulation can also lead to collective harms beyond the consumer realm, such as threats to democracy and freedom of expression (Susser, Roessler and Nissenbaum, 2019[108]).

Personal consumer detriment

The dark patterns literature has highlighted personal detriment as the primary normative concern about dark patterns (Mathur, Kshirsagar and Mayer, 2021[53]). The personal consumer detriment from dark patterns can be broadly divided into three broad categories: i) financial loss, ii) privacy harms, and iii) psychological detriment and time loss. These harms are likely to be cumulative where multiple dark patterns are employed at once and are often interrelated (e.g. financial and privacy loss can also lead to psychological detriment).[17]

Financial loss

Financial loss is the most commonly identified welfare consequence of dark patterns in the literature (Mathur, Kshirsagar and Mayer, 2021[53]). Dark patterns such as sneak into basket, hidden costs, drip pricing or scarcity cues are clearly aimed at getting consumers to buy something that they may not have needed or to spend more than they may have otherwise intended. Some dark patterns may more indirectly lead consumers to incur financial losses, such as preselection (e.g. a more expensive variant is pre-selected), urgency-related dark patterns (e.g. the consumer is pressured into buying a product they may not have needed), or confirmshaming (e.g. the consumer is shamed into maintaining a subscription they may not need). For dark patterns such as hidden or hard to cancel subscriptions, the unintended financial expenditure may occur on an ongoing basis and could amount to significantly larger losses than those incurred from one-off purchases.

To date there is no comparative assessment of the financial losses that different dark patterns may cause, and doing so may prove challenging as the magnitude of detriment measured resulting from different dark patterns may be highly dependent on the methodological set-up. Nonetheless, research and enforcement actions have shed light on the substantial financial detriment resulting from specific dark patterns, in particular *hidden costs / drip pricing* and *subscription traps*. For example, Blake et al. (2021[109]) found that use of drip pricing resulted in consumers spending 21% more than otherwise. Action by the US FTC in 2020 against an online business for automatic renewal of consumers' subscriptions without proper consent led to USD 9.7 million in refunds to consumers affected by the practice in 2021.[18] Other evidence points to the financial loss resulting from a combination of dark patterns. For example, the CMA's investigation into hotel booking sites in 2017, for misleading activity messages and scarcity claims, misleading discount claims, incorrect reference pricing and hidden charges, led to the subsequent alignment of such practices with UK consumer laws with benefits to consumers estimated at GBP 34 million (OECD, 2021[9]). In an experiment by the French consumer protection authority (DGCCRF), 2 542 consumers were tricked into buying a fake coffee machine as a result of Facebook advertisements featuring dark patterns, which would have resulted in total losses of EUR 150 000 for such consumers over the course of less than four weeks (DITP & DGCCRF, 2021[111]). Consumer survey data also confirm the financial impact of dark patterns in general on consumers (CPRC, 2022[112]). Annex E provides an overview of evidence of financial loss resulting from certain dark patterns.

But for many other dark patterns, concrete evidence of financial detriment is lacking. One reason may be that consumer authorities have long recognised subscription traps and drip pricing as problematic, which may have driven an earlier need to gather evidence on the detriment they cause and take enforcement action. Another may be that some dark patterns are less amenable to assessing the magnitude of associated financial losses, especially if the detriment remains hidden to the consumer. For example, consumers might be induced to pay more for a product than they otherwise would as a result of confirmshaming, trick questions or false hierarchy dark patterns, without appreciating the extent of the financial loss associated.

Privacy harms

The academic literature, as well as a range of stakeholders including legislators (see Section 5 for more details), data protection regulators (CNIL, 2019[113]), or consumer organisations (Forbrukerrådet, 2018[27]; Forbrukerrådet, 2018[84]), have also emphasised the privacy concerns of dark patterns (Mathur, Kshirsagar and Mayer, 2021[53]). Key examples of privacy-intrusive dark patterns are those that set privacy-intrusive settings as the default (e.g. preselection), that make privacy-related choices or information hard to engage with or opt out of (forced disclosure, hidden information, hard to cancel), or that nag or shame the consumer into accepting privacy-intrusive settings (nagging, confirmshaming). As a result, consumers may end up divulging more personal data than intended, potentially exposing them to further risks. A survey of Australian consumers found one in four shared more personal information than desired owing to dark patterns (CPRC, 2022[112]).

But assessing the magnitude of privacy harms of dark patterns is more challenging than it is for their financial detriment as a quantifiable indicator is lacking. Indeed courts tend to struggle to recognise privacy harms as they are often not associated with tangible financial or physical harm (Citron and Solove, 2022[114]). Moreover, consumer complaints may be lacking where consumers are unaware that their privacy has been affected. Consumers may also have difficulty assessing the harm resulting from a transaction involving their personal data, because the trade-off between the tangible and immediate short-term benefit of using the service and the costs of potential long-term privacy loss is difficult to evaluate (Forbrukerrådet, 2018[27]).

To the extent that consumers can be considered to "pay" for non-monetary online transactions by bartering their personal data or attention time (Stigler Committee, 2019[49]), some scholars have conceptualised the detriment from privacy-intrusive dark patterns as a higher "data price" than they would freely choose in exchange for the quality of the service (Morton and Dinielli, 2020[115]). [19] Specifically, consumers that fall prey to privacy-intrusive dark patterns may be paying more in data or attention for a zero-price online service, and be served welfare-reducing advertisements for no corresponding increase in quality. Alternatively, Gunawan, Choffnes and Wilson (2021[115]) suggest that measuring the level of effort required to avoid a privacy-intrusive dark pattern could provide insight into the magnitude of its harm. A typology of privacy harms also shows that there are several other ways they may be cognisable and thus potentially assessable, including in terms of reputational, emotional, discrimination, informed choice and autonomy harms (Citron and Solove, 2022[114]).

Psychological detriment and time loss

The psychological detriment caused by dark patterns relates to emotional distress, such as frustration, feelings of shame and being tricked,[20] and the cognitive burden of unnecessarily expending energy or attention (Mathur, Kshirsagar and Mayer, 2021[53]), which may lead to time loss. Frustration and cognitive burden might result from exploiting consumers' inertia or limited willpower, attention span or time, for example by repeatedly prompting the consumer to agree to certain settings (nagging), making it harder to cancel than to sign up or to select the appropriate choice (trick questions).

Dark patterns that manage to sufficiently capture the consumer's attention and time for extended durations may be considered addictive. The Stigler Committee (2019[49]) submits that the business model of major online platforms is based on addictive user interface designs to maintain consumer attention. Certain kinds of user interface design practices that are commonplace on social media platforms, such as the infinite scroll and autoplay designs, have been found by researchers to trigger addictive usage patterns among consumers (Purohit, Barclay and Holzer, 2020[116]). In video games, loot boxes have been considered to incorporate dark patterns that cause addiction, particularly for children (Forbrukerrådet, 2022[90]). They have been characterised as a form of "gamblification" due to their usage of elements typically seen in slot machines (Goodstein, 2021[89]) and as "predatory monetisation schemes" as they disguise their long-term cost until players are already financially and psychologically committed (King and Delfabbro, 2018[118]).

Various studies focusing on end-user experiences have shown that dark patterns cause negative emotional and physiological reactions in consumers. Several surveys found consumers subjected to dark patterns became significantly upset, annoyed and frustrated or felt manipulated (Luguri and Strahilevitz, 2021[25]; Voigt, Schlögl and Groth, 2021[118]; CPRC, 2022[111]). Research by Gray et al. (2021[119]) showed that consumers frequently felt strong emotions such as distress, hostility and irritability when subjected to manipulative digital product experiences. In relation to specific dark patterns, Conti and Sobiesk (2010[22]) found that all malicious interface techniques they assessed caused significant frustration to respondents, with "installation of applications without permission", "unnecessary interruptions", "difficult to find content" and "forced waiting" being among the most frustrating techniques. In research by Shaw (2019[120]), a third of survey respondents exposed to scarcity and social proof claims on hotel booking sites expressed negative reactions such as contempt and disgust; likewise, Kristofferson et al (2017[121]) found scarcity cues led to aggression. The 2022 EC study established that some dark patterns led to increases in heart rate, more rapid eye movement, erratic mouse clicks, potentially indicating greater anxiety and alertness (EC, 2022[29]). But not necessarily all dark patterns cause an emotional reaction; for example, both Luguri and Strahilevitz (2021[25]) and the 2022 EC study (EC, 2022[29]) found confirmshaming to have no effect on mood, and explained this as some level of habituation to the practice.

Studies have also shown that consumers tend to attribute blame to businesses for use of dark patterns. Specifically, Bhoot, Shinde and Mishra (2020[104]) and Maier and Harr (2020[103]) found consumers primarily blamed business owners for employing dark patterns. Gray et al. (2021[119]) found most consumers blamed the designer, developer or other stakeholders for manipulative experiences in digital products, with a minority blaming themselves.

Annex E provides further details on the existing research identified relating to psychological detriment from dark patterns.

Structural consumer detriment

Dark patterns may cause structural consumer detriment by having a cumulative impact on consumers collectively, even where they have imperceptible harms at the individual level. Such impacts can be explored from a number of perspectives, in particular in terms of impacts on competition and consumer trust and engagement in the market (Mathur, Kshirsagar and Mayer, 2021[53]).[21]

Weaker or distorted competition

The use of dark patterns can undermine competition in several ways. Some dark patterns may affect competition by hindering or disincentivising the process of shopping around and comparing offers. Drip pricing, for example, through reduced price transparency, has been found to hinder consumers' ability to identify the lowest price (Rasch, Thöne and Wenzel, 2020[123]). Additional examples include default preselection, price comparison prevention, and scarcity cues. Other dark patterns may more concretely lock consumers into existing services and hamper switching, such as the forced registration, hidden subscription and hard to cancel dark patterns. The ACCC has for example recently identified dark patterns that hinder switching of browsers (ACCC, 2021[88]).

Firms employing dark patterns may also be able to extract more sales (e.g. through drip pricing), personal data (e.g. through privacy-intrusive defaults) or attention time (e.g. through addictive practices), thereby obtaining a competitive advantage over firms that do not employ dark patterns, without offering better quality goods or services. Dominant firms may use dark patterns to further entrench their market position. For example, some dark patterns may be used to neutralise competitive threats (e.g. through preselected defaults (CMA, 2022[31]) or nagging (Hung, 2021[56])), or to gather consumer data to offer services in ways that rivals cannot (e.g. in a more personalised manner) (OECD, 2020[124]; Slaughter, 2021[125]; Kemp, 2020[43]). A dominant firm could also use dark patterns to leverage its position to obtain market power in a related or downstream market (Day and Stemler, 2020[126]), which is how some commentators have understood Google's conduct in the EC's self-preferencing case *Google Shopping* (Himes and Crevier, 2021[127]).

To the extent dark patterns impede consumers' ability to select the best firms on the merits of their product offerings, market use of dark patterns can distort the competitive process as a whole (Kemp, 2020[43]; Day and Stemler, 2020[126]). Market efficiency can suffer in particular through the transaction costs some dark patterns impose (Stigler Committee, 2019[49]), such as the costs of evaluating the advantages and disadvantages of different choices (e.g. drip pricing, hidden information) or the costs of implementing such choices (e.g. hard to cancel, subscription traps) (Shahab and Lades, 2021[128]). Furthermore, as discussed in Section 2, competitive pressures may lead some businesses to routinely use and thus come to rely on dark patterns where they are not clearly prohibited. Economists have notably highlighted the risks of a sub-optimal "phishing equilibrium" when businesses are forced to use deceptive methods to compete, as a result of a combination of information asymmetry and behavioural market failure (Akerlof and Shiller, 2016[129]; Willis, 2020[39]). In the context of dark patterns, an inefficient market equilibrium may result where firms also compete through the effectiveness of their dark patterns, including particularly salient aspects of a user interface design, rather than purely on the price and quality of their products (CMA, 2021[19]). In the case of drip pricing, for example, businesses may be less likely to compete on mandatory add-ons due to their lack of salience (CMA, 2022[31]).

Less consumer trust and engagement

Much of consumers' behaviour towards online businesses is based on trust, which has been defined as expectations that businesses will behave in a favourable, predictable manner (Waldman, 2020[130]). To the extent that dark patterns may trick consumers into divulging more personal information or paying more than desired, they may sow distrust in online businesses that employ them (if consumers do become aware of them).

Maier and Harr (2020[103]) found consumers' trust in a company is weakened and its credibility compromised if it employs too many manipulative techniques. Voigt, Schlögl and Groth (2021[118]) found a significant connection between consumer annoyance resulting from dark patterns and their trust in a brand. Other research sheds light on the effects of specific dark patterns. Shaw (2019[120]) found almost half of consumers exposed to scarcity and social proof claims on hotel booking sites distrusted the sites as a result. Robbert and Roth (2014[130]) found that drip pricing led consumers to feel deceived by sellers and perceive such pricing practices as unfair. Similarly, Totzek and Jurgensen (2021[131]) found that drip pricing lowered perceived price fairness by increasing consumers' attention to the final price, particularly when the number of surcharges was high, as well as because of higher perceived price complexity and lower pricing transparency perceptions.

Over time, lack of trust resulting from dark patterns may lead consumers to lose faith in markets and market forces and disengage (Luguri and Strahilevitz, 2021[25]). Indeed survey data has shown consumers may temporarily or permanently cease using websites or apps (CPRC, 2022[112]). Even if consumers learn to resist dark patterns such as false countdown timers, such resistance may also lead consumers to disengage when faced with genuine time-limited deals, potentially harming honest businesses (Mathur, Kshirsagar and Mayer, 2021[53]). Disengagement can further compromise healthy competition to the extent consumers cease to shop around and discipline dishonest businesses (Siciliani, Riefa and Gamper, 2019[133]).

See Annex E for further details on selected evidence of impacts of dark patterns on consumer trust.

Consumer vulnerability to dark patterns

As dark patterns can be designed to exploit certain cognitive and behavioural biases so as to lead consumers into making a decision that they may not otherwise have made, consumers are inherently more vulnerable to dark patterns than other commercial practices that do not bear the same possibility of consumer manipulation (OECD, 2021[9]). A 2016 EC study notes dark patterns, such as drip pricing and time-limited offers, specifically target "behavioural drivers of vulnerability" (EC, 2016[134]).

Furthermore, many stakeholders have recognised the heightened vulnerability to dark patterns of certain subsets of consumers, and some suggest that this is what warrants the urgency to regulate them (Chugh and Jain, 2021[135]). For instance, in relation to dark patterns that unnecessarily impose transaction costs such as making it difficult to opt out, the Stigler Committee (2019[49]) note that "users who are less tech savvy or do not have the extra time to devote to navigating byzantine opt out procedures will be less likely to persist so that they can express their authentic preferences in the transaction. Further, these groups may preferentially include those who are already at some social disadvantages, such as elderly people with less developed technology skills or less educated people." Also, Radesky (2021[135]) considers that five differences from adults make children more susceptible to dark patterns: having immature executive function; forming imaginative relationships with characters; being susceptible to rewards; being indifferent or unfamiliar with data privacy; and lack of understanding of virtual currencies.

Some empirical evidence illustrates how dark patterns may affect certain groups of consumers more than others. Luguri and Strahilevitz (2021[25]) demonstrated that less educated consumers were significantly more susceptible to "mild" or subtle dark patterns than better educated consumers. Bongard-Blanchy et al. (2021[33]) found that both people over 40 as well as people possessing only high school diplomas were less likely to recognise dark patterns. Similarly, the 2022 EC study found that dark patterns were more effective on older age and less educated consumers as well as those who were in a situation of transitory vulnerability as a result of time pressure to make a choice (EC, 2022[29]). In contrast, the Consumer Policy Research Centre (CPRC) (2022[111]) found in a survey that consumers of age 18 to 28 years were more likely to be negatively impacted by dark patterns than any other age group, and were 65% more likely to spend more than intended owing to dark patterns. Furthermore, children have been shown to be particularly prone to be affected by dark patterns in advertising in apps (Meyer et al., 2019[137]) and in the design of loot boxes in online games (Forbrukerrådet, 2022[89]), particularly where they incentivise spending and personal data sharing (Bell and Fitton, 2021[138]). Radesky et al (2022[58]) furthermore found children of families of low socio-economic status were more likely to encounter manipulative design features in children's apps.

Specific cases of dark patterns have also shed light on the susceptibility of certain consumer groups. Both the EC together with national EU consumer authorities[22] as well as the US FTC[23] have taken action against major online platforms for user interface designs in child-directed "free" apps that resulted in children inadvertently racking up charges without parents' knowledge or authorisation. Furthermore, US tax software company TurboTax was alleged to use dark patterns to hide the option of filing taxes for free, despite this being a right under US law for people earning an income below a certain threshold, thus disproportionately impacting low-income consumers.[24]

Dark patterns documented in the literature to date operate in the same way for all consumers, irrespective of their personal attributes or behaviours (Narayanan et al., 2020[34]). Nonetheless, some researchers predict that over time, businesses will increasingly be able to personalise dark patterns, making it easier to target consumers' vulnerabilities with a high level of granularity (Luguri and Strahilevitz, 2021[25];

Helberger et al., 2021[138]; Stigler Committee, 2019[49]; EC, 2022[29]). Specifically, it is argued businesses may be able to target consumers with the dark patterns to which they may be most vulnerable, for instance based on data concerning e.g. where they live (e.g. residents of a retirement village, or people from certain language backgrounds), whether they suffer from a specific health-related vulnerability (e.g. mental illness), or are in a specific emotional or physiological state (e.g. bereavement). These possibilities may expand the traditional notion of "vulnerable consumers" beyond a group defined by demographic factors to a broader set of circumstances (Fletcher et al., 2021[139]). The CCP's report "Consumer Vulnerability in the Digital Age" further discusses changes in the nature and extent of consumer vulnerability in the digital age as a result of emerging digital trends and implications for consumer policy (OECD, forthcoming[10]).

5. Regulatory and enforcement measures to address dark commercial patterns

Key points

- Market forces alone are unlikely to address dark patterns satisfactorily, and may further incentivise use of dark patterns.
- Many consumer and data protection authorities have taken enforcement actions and consumer organisations have filed complaints about the use of dark patterns. But enforcement cases to date predominantly relate to a limited set of dark patterns commonly recognised by regulators. This may indicate possible gaps in the law, available evidence, or enforcement capacity. In particular, some dark patterns that are not clearly deceptive may not be captured by existing general prohibitions on deceptive commercial practices.
- Various regulatory measures to respond to dark patterns have been proposed or implemented across OECD jurisdictions. These include measures to: address them specifically on online platforms; prohibit specific kinds of dark patterns; foster consumer-friendly digital choice architecture (such as by making it as easy to cancel or opt out as to sign up or opt in); further empower regulators; and address consumer vulnerability. Guidance has also been issued in several jurisdictions to assist businesses' compliance with relevant laws.
- However, a wealth of evidence indicates that disclosure and transparency measures are not sufficient in isolation to protect consumers from dark patterns and that, if employed, their design should be carefully considered taking into account available empirical evidence.
- Other key considerations relate to combining principle- and rule-based regulation in the design of consumer law; employing specific tools to gather evidence and inform policy and enforcement (including web scraping); enhancing co-operation among relevant policy areas (e.g. privacy, competition policy and AI); and adapting interpretation of legal standards.
- Empirical evidence reviewed for this report suggests policy and enforcement focus could be applied to tackling dark patterns on apps and mobile devices, on major platforms and popular e-commerce websites and apps, instances of combined or layered dark patterns, and third-party entities enabling creation of dark patterns. Other priorities could include protecting more vulnerable consumers and developing requirements to foster consumer-friendly digital choice architecture. Furthermore, given the demonstrated high prevalence in several areas, effectiveness in influencing consumer behaviour and ability to avoid detection of the hidden information, false hierarchy, preselection and hard to cancel/opt out dark patterns, policy and enforcement efforts could focus on them as a priority – while continuing to gather evidence on other dark patterns.

Existing laws and enforcement actions to address dark patterns

There is broad consensus among scholars that market forces alone are unlikely to address dark patterns satisfactorily, and that competitive markets may in fact incentivise more, rather than less usage of dark patterns (as discussed in Section 2) (Stigler Committee, 2019[49]). Consumer and data protection authorities have accordingly been active in addressing dark patterns on the basis of relevant laws. These include principle-based or specific consumer protection laws prohibiting misleading, deceptive or unfair practices associated with many dark patterns, or data protection laws requiring transactions to be conducted with appropriate levels of transparency or consent that may not be compatible with certain dark patterns; indeed, as discussed in Section 3, many cookie consent notices featuring dark patterns are likely to be clearly in breach of data protection laws in certain jurisdictions. The below provides examples of such laws and enforcement action from selected OECD jurisdictions.

Existing laws addressing dark patterns in selected OECD jurisdictions

The EC and ACM advise that the principle-based prohibitions in the EU UCPD on practices that are deemed unfair – because either they both materially distort the economic behaviour of the average consumer and are contrary to the requirements of professional diligence (Article 5); are misleading actions or omissions (Articles 6 and 7); or are aggressive practices (Articles 8 and 9) – could each apply to various dark patterns (EC, 2021[141]; EC, 2022[29]; ACM, 2020[20]). Annex I of the UCPD also contains a list of specific blacklisted practices, many of which would also apply to specific dark patterns (EC, 2021[141]; EC, 2022[29]). For example, blacklisted practice no.7 relates to false limited-time statements (relevant for false countdown timers); no.11 to use of editorial content in the media for advertising without making that clear in the content (relevant for disguised ads); no. 18 to materially inaccurate statements about market conditions (relevant for false low-stock messages); and no. 26 to persistent and unwanted solicitations by remote media (relevant for nagging). Dark patterns targeting vulnerabilities of individual or specific groups of consumers could potentially also amount to a form of manipulation in which the trader exercises "undue influence" over the consumer, which is an aggressive practice prohibited under Articles 8 and 9 (EC, 2021[141]).

In addition to the UCPD, the EC and other stakeholders and researchers have suggested that many dark patterns are likely to fall foul of several other EU laws, including the GDPR (relevant to several privacy-intrusive dark patterns); the Consumer Rights Directive 2011/83/EU (relevant to e.g. hidden costs / drip pricing and hidden subscriptions); the Unfair Contract Terms Directive 93/13/EEC (relevant to e.g. hard to cancel); and the Audiovisual Media Services Directive 2010/13/EU (relevant to disguised ads) (EC, 2022[29]; EC, 2021[140]; BEUC, 2022[141]; Leiser, 2020[48]; Berbece, 2019[142]). Annex F provides an overview of EU legislation, based on the 2022 EC study (EC, 2022[29]), that may be relevant for addressing different dark patterns. Similarly, the UK Consumer Protection from Unfair Trading Regulations 2008 (CPRs) contain principle-based prohibitions (Part 2), as well as a list of practices that are in all cases prohibited (Schedule 1), both of which largely mirror the UCPD, while the UK Data Protection Act 2018 defines consent in the same way as the GDPR.

In the US, Section 5 of the Federal Trade Commission Act (FTC Act, 15 U.S.C. § 45) contains principle-based prohibitions on deceptive and unfair acts or practices. The FTC considers a deceptive act or practice to be any representation, omission, or practice that is both (i) material and (ii) likely to mislead consumers who are acting reasonably under the circumstances (US FTC, 1984[144]). An unfair trade practice is defined (differently from an unfair commercial practice in the EU UCPD) as one that (i) causes or is likely to cause substantial injury to consumers, (ii) is not reasonably avoidable by consumers themselves and (iii) is not outweighed by countervailing benefits to consumers or competition. US law also provides for express prohibitions on specific practices found in dark patterns, such as on bait and switch practices (16 CFR § 238), on continuing to charge a consumer for a good or service after an initial transaction without the consumer's express informed consent (Restore Online Shoppers' Confidence Act, 15 U.S.C. §§ 8401-8405), and on making it hard to opt out of marketers' emails (CAN-SPAM Act, 15 U.S.C. § 7704(a)).

Several commentators have noted that many dark patterns are illegal under such US federal laws, or under US state laws prohibiting deceptive and unfair practices (Luguri and Strahilevitz, 2021[25]; Willis, 2020[39]; Fletcher et al., 2021[139]; Warner, 2021[144]; Kaufman, 2021[145]). For example, the FTC has used Section 5's prohibition on deceptive acts in commerce to challenge hard to cancel, hidden costs, forced continuity, hidden information, preselection, trick questions and disguised ads dark patterns (Luguri and Strahilevitz, 2021[25]; US FTC, 2022[146]). According to Luguri and Strahilevitz (2021[25]), false activity messages, sneak into basket, bait and switch, forced registration, and scarcity-related practices might also be seen as deceptive acts. Techniques that are not obviously deceptive, such as nagging, price comparison prevention, intermediate currency, toying with emotion, or confirmshaming could potentially be challenged under the prohibition on unfair trading practices, though this approach remains untested (see also further discussion below) (Luguri and Strahilevitz, 2021[25]; Stigler Committee, 2019[49]).

As a further example, the Australian Consumer Law (ACL), in Schedule 2 of the Competition and Consumer Act 2010, contains general protections against misleading or deceptive conduct, unconscionable conduct and unfair contract terms that could be employed against dark patterns. It also contains specific protections against a range of practices that may be involved in certain dark patterns, such as demanding payment for an unsolicited good or service (e.g. sneak into basket), not prominently displaying the total price of a good or service (e.g. hidden charges / drip pricing), or bait advertising (bait and switch) (Temby and Vasquez, 2020[147]).

To the extent dominant firms use dark patterns, as discussed in Section 4, competition law relating to abuse of dominance may also be a tool through which to address them. For example, the use by a dominant firm of privacy-intrusive dark patterns to collect personal data above competitive levels could be seen as a form of exploitative conduct that may contravene laws against the abuse of dominance in jurisdictions in which exploitative conduct constitutes such an abuse (e.g. in the EU under Article 102 of the Treaty on the Functioning of the European Union and other similar national laws) (Kemp, 2020[43]). Dark patterns that serve to exclude rivals could also amount to exclusionary single-firm conduct, which may contravene competition laws in several jurisdictions (e.g. the laws against monopolisation in the US or misuse of market power in Australia) (Kemp, 2020[43]; Day and Stemler, 2020[126]).

Enforcement actions and legal complaints regarding dark patterns in selected OECD jurisdictions

Consumer and data protection authorities in the jurisdictions discussed above as well as in numerous other OECD jurisdictions have used their authority to take enforcement action under relevant laws and consumer organisations have filed legal complaints against use of dark patterns, without necessarily referring to them as such. Annex G provides a non-exhaustive overview of examples. Enforcement actions cover a range of options from the enforcement toolbox, including persuasion and negotiation, warning letters, out-of-court settlements, civil penalties and bans.

A key takeaway is that in many jurisdictions, consumer and data protection authorities already have the tools to address dark patterns. Nonetheless, most of the cases identified relate to a limited set of dark patterns, such as hidden charges/drip pricing, subscription traps, false scarcity claims and preselection of privacy-intrusive settings. Cases addressing the panoply of other dark patterns, such as trick questions, confirmshaming/toying with emotion, nagging, price comparison prevention, immortal accounts and intermediate currency, appear rare.

Several reasons might explain this disparity. One is that for some dark patterns there is insufficient evidence of violations of relevant laws or of consumer detriment resulting from some dark patterns to take enforcement action. This may be because of insufficient investigative powers or tools, or because detriment may remain hidden to consumers, especially in cases of more subtle dark patterns. Another reason is a lack of resources: with the plethora of dark patterns and other malicious practices online, resourced-constrained consumer and data protection authorities may be obliged to prioritise their enforcement activities on clearly egregious misconduct. Indeed, the 2022 EC study confirms that there is a need for more enforcement of EU consumer law against dark patterns, and recommends improving the resources and powers of enforcement authorities (EC, 2022[29]). Further reasons may be that some authorities are yet to recognise the dangers of dark patterns or that investigations may be ongoing and not yet public.

But another possible explanation is that such practices may not be clearly unlawful under existing laws in some jurisdictions, such as general misconduct prohibitions, and/or present a high evidentiary burden under such laws. Various commentators have suggested that in particular dark patterns that are not clearly deceptive – in the sense that they do not necessarily cause a consumer to believe something that is not true – are unlikely to be captured by prohibitions on misleading or deceptive conduct as formulated in certain jurisdictions (CPRC, 2020[148]; King and Stephan, 2021[149]; ACCC, 2021[88]; Chugh and Jain, 2021[135]). Indeed, in their review of US case law, Luguri and Strahilevitz (2021[25]) did not identify cases indicating whether practices that do not clearly constitute deceptive acts, such as nagging, price comparison prevention, intermediate currency, toying with emotion or confirmshaming, were unlawful. They also found little US case law discussing unfairness and dark patterns in depth, and suggest, in line with Calo (2014[18]), that some dark patterns might not meet the requirements of an unfair trade practice under the FTC Act; Hung (2021[56]) asserts that nagging in particular would most likely not such requirements. Similarly, commentators have suggested that there may be no obvious provision in the ACL that would protect against the hard to cancel dark pattern, particularly as it may not necessarily be misleading or deceptive to make it easier to sign up to a service than to cancel it (Temby and Vasquez, 2020[147]). Such a distinction between clearly deceptive and more subtle dark patterns may also reflect that it may be more straightforward to establish the deceptiveness of text than certain non-text design features.

Emerging regulatory responses and proposals to address dark patterns

Despite relevant existing laws, a number of government bodies have proposed or implemented new regulatory measures to address dark patterns, and academia and consumer organisations have similarly put forward reforms. Some are considering doing so pending further evidence. For example, following the update of its guidance documents on the UCPD and CRD in 2021, in 2022 the EC announced a "fitness check" (i.e. an evaluation of a group of related policy interventions) to examine the adequacy of the UCPD, CRD and UCTD in the digital environment, including to protect consumers from dark patterns.[25] Likewise, in 2022, the UK government announced that it would continue to build its evidence base to inform possible strengthening of the law to allow the CMA to more easily take action against exploitative designs using behavioural techniques on websites to influence consumers,[26] including by adding to the list of blacklisted practices in Schedule 1 of the CPRs as well as further promoting "fairness by design" principles (UK BEIS, 2021[150]).

The following details recent and emerging regulatory proposals and responses from selected jurisdictions by theme.

Addressing dark patterns on online platforms

Much of the focus of proposals to further regulate dark patterns has centred on online platforms, in consideration of the significant role they play in the digital economy, including in terms of scale and access to data and power imbalances with respect to consumers. Such proposals have mixed negative obligations to avoid dark patterns, positive obligations to ensure consumer-friendly choice architecture and requirements regarding the platform's conduct of experiments (including A/B testing) on consumers.

In particular, the EU Digital Services Act (DSA) and Digital Markets Act (DMA) adopted in 2022 will place new obligations and prohibitions on online platforms in the EU. As discussed in Box 2 of Section 2, the DSA will prohibit online platforms from designing, organising or operating online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of recipients of their service to make free and informed decisions. The DSA further provides that the EC may issue guidance on how the prohibition applies in relation to specific dark patterns – particularly false hierarchy, nagging and hard to cancel[27] – and that the prohibition does not apply to practices already covered by the UCPD and GDPR (EP, 2022[54]). The DMA will furthermore prohibit the use of dark patterns to circumvent the obligations it lays down on online platforms with a systemic role in the EU internal market ("gatekeepers") (EP, 2022[55]).

Legislative proposals regulating dark patterns on online platforms have also been introduced in other jurisdictions (but had not passed at the time of writing). Specifically:

- In 2019, senators in the US first introduced the DETOUR Act, which would prohibit large online platforms from using dark patterns (as set out in Box 2) to trick consumers into giving up their personal data.[28] In addition, it would prohibit such platforms from subdividing or segmenting consumers for the purposes of behavioural experiments without a consumer's informed consent and require large online operators to create an internal Independent Review Board to provide oversight on such practices to safeguard consumer welfare.[29]
- In 2019, senators in France introduced a bill to the Senate, "Proposition de loi visant à garantir le libre choix du consommateur dans le cyberspace" (Proposal for a law to ensure free consumer choice in cyberspace), of which a later version (2020) contained provisions to prohibit online platforms from designing, modifying or manipulating a user interface with the purpose or effect of subverting or altering the autonomy of the consumer in making a decision or of obtaining their consent.[30].

In 2020, the CMA recommended the introduction of a "fairness by design" duty on online platforms to complement the GDPR's "data protection by design" duty. The high-level principles-based duty would require platforms to design choice architecture in a way that encourages free and informed consumer choice over the use of their personal data. Platforms would be required to demonstrate compliance with the duty (CMA, 2020[86]). The ACCC considered that a similar broad, principles-based obligation requiring platforms to present information and choices in a way that is accessible, balanced, and empowers consumers to exercise their settings and controls, subject to oversight by an external body, should be considered in Australia (ACCC, 2021[88]), which could address the false hierarchy, nagging and hard to cancel dark patterns, for example (ACCC, 2022[151]).

Researchers have supported these and similar such proposals. Fletcher et al. (2021[139]) consider the largest online platforms should be given specific responsibility to ensure their choice architecture is neutral and Costa and Halpern (2019[151]) propose specific governance and oversight mechanisms for platforms. In the same vein, the Stigler Committee (2019[49]) propose imposing "consumertarian" default rules that are "sticky," i.e. rules imposing default settings for which there are stringent constraints on waiving the default in favour of a less data protective or otherwise consumer-friendly setting. Other researchers have proposed special kinds of obligations on online platforms or online businesses in general to address dark patterns, such as an ethical code (Stemler, Perry and Haugh, 2020[153]), a positive duty of forthrightness (Ohm, 2018[154]) or a universal service framework (Helberger et al., 2021[139]).

Similar to the proposed US DETOUR Act, Fletcher et al. (2021[139]) and the Stigler Committee (2019[49]) suggest the implementation of rules governing access to and transparency of the results of consumer experimentation (A/B testing) of large online platforms, including requiring platforms to make their results available to regulators and researchers to identify potential dark patterns.

Prohibiting specific kinds of dark patterns

A range of responses have also been put forward or implemented to prohibit use of specific dark patterns, not only by online platforms but online businesses in general. For example, several consumer protection researchers have proposed banning the use of defaults that require a consumer to "opt out" in order to avoid a financial commitment; banning messages that create a false sense of urgency or scarcity; requiring that prices be displayed prominently upfront and include all unavoidable fees and charges; prohibiting interface design which acts to misdirect consumers; and regulating fake reviews, friend spam, subscription traps and privacy-intrusive dark patterns (Fletcher et al., 2021[139]). Many of these proposals have already been implemented in some form in OECD jurisdictions; where they have not, the researchers suggest many could be enacted through minor changes to existing law or regulation or through decisional law interpreting existing standards of conduct (Fletcher et al., 2021[139]). Though other proposals may be more aspirational, requiring more analysis of enforceability and unintended consequences.

In some cases, measures proposed for online platforms could be considered for online businesses more broadly. For example, participants at the European Consumer Summit 2022[31] raised the option of extending prohibitions on dark patterns in the DSA to online businesses in general in the UCPD (EC, 2022[155]).

The following provides further details on selected measures to prohibit specific kinds of dark patterns.

"Unfair" and "abusive" dark patterns

As discussed above, while many OECD jurisdictions include principle-based prohibitions on deceptive commercial practices in their consumer laws, some kinds of dark patterns may not clearly constitute deceptive acts (e.g. confirmshaming or nagging). This has led to some calls for other forms of principle-based prohibitions to be introduced, which, depending on how they are formulated, may provide the legal authority to address such dark patterns.

In Australia, for example, where a general prohibition on unfair trading practices is absent, the ACCC and other commentators have proposed the introduction of a carefully defined and targeted provision prohibiting unfair trading practices to help address dark patterns that significantly impede consumer choice and cause harm.[32] (ACCC, 2021[88]; Paterson and Bant, 2020[156]; CPRC, 2020[148]).

Furthermore, in the US, some scholars have suggested there be a prohibition on "abusive" practices, mirroring an existing prohibition in US financial consumer protection law,[33] to address dark patterns that may not meet the bar of deceptive or unfair practices as defined in the US FTC Act (see examples discussed above) (Hoofnagle, Hartzog and Solove, 2019[157]; King and Stephan, 2021[149]). Researchers suggest such a prohibition could particularly capture dark patterns that exploit cognitive biases of consumers in order to manipulate them (Luguri and Strahilevitz, 2021[25]) or "that take unreasonable advantage of people's understanding, limited abilities, or reliance on relationships and transaction costs" (Hartzog, 2018[158]) (which may apply to nagging (Hung, 2021[56]), among other dark patterns). To the extent the formulation of a prohibition on abusive practices were to bear similarity to the EU UCPD's prohibition on aggressive practices (Articles 8 and 9), it may also capture the same dark patterns that the latter is deemed to, such as nagging and confirmshaming (see Annex F).

Hard to cancel/opt out and hidden subscriptions

A number of jurisdictions have introduced or announced consideration of laws to better combat dark patterns that make it hard to cancel or opt out of certain settings or transactions, including subscription traps. For example, in 2020 Argentina introduced a regulation requiring businesses to prominently display a button for consumers to easily cancel the online purchase of goods or services, without any further procedures.[34] Similarly, in 2021 Germany introduced a law (Fair Consumer Contracts Act), which took effect in July 2022, requiring businesses to provide a specifically labelled button leading to a contact form through which consumers can cancel existing subscriptions with the click of only one further button.[35] Various states in the US have in recent years enacted laws strictly regulating the use of auto-renewal clauses in business to consumer contracts.[36] In 2022, the UK government announced it would introduce measures to better tackle subscription traps, including by requiring that consumers be able to exit a contract through a straightforward, cost-effective and timely mechanism.[37]

In 2021, regulations in California amended the California Consumer Privacy Act (CCPA) to ban dark patterns that subvert or impair a consumer's choice to opt out of schemes where their personal data is sold. The practices covered by the ban included requiring consumers to go through several steps or pages before submitting a request to opt out as well as trick questions (double negatives).[38]

Further, the FTC released an enforcement policy statement in 2021 clarifying that under FTC law businesses' sign-up process for subscription services must provide clear, up-front information, obtain consumers' informed consent, and make cancellation easy (US FTC, 2021[159]). In a similar vein, both the EC and CMA encourage businesses to ensure unsubscribing from a service/exiting a contract is as easy as subscribing/entering (EC, 2021[141]; CMA, 2018[160]). The French data protection authority (CNIL) also clarified, in a recommendation, that to ensure compliance with the GDPR a consumer should be able to reject cookies and tracking as easily as accept them, with buttons of equal visual prominence (CNIL, 2020[161]) (see also further discussion of regulatory guidance below).

Researchers and consumer organisations have echoed such proposals (Costa and Halpern, 2019[152]; Forbrukerrådet, 2021[87]) and advocacy efforts launched by the Norwegian Consumer Council have led to a change in business practices in European jurisdictions.[39] The European Consumer Organisation (BEUC) furthermore proposed that the German Fair Consumer Contracts Act be replicated at EU level in the CRD (BEUC, 2022[141]).

Consent-related dark patterns

In 2020, in California the California Privacy Rights Act (CPRA) amended the CCPA with new laws to take effect on 1 January 2023. The amendments introduced a definition of dark patterns (as noted in Box 2), and provided that "consent obtained through dark patterns does not constitute consent" (CPRA/ Cal. Civ. Code § 1798.140(l)). Similar amendments to privacy laws have been introduced in other states, or were under consideration at the time of writing.[40]

In the same vein, a bill introduced in Canada in 2022, the Digital Charter Implementation Act (Bill C-27), would prohibit and invalidate consent obtained through false or misleading information or use of deceptive or misleading practices, which is considered to cover dark patterns.[41]

In 2017, the EC proposed the ePrivacy Regulation, which would further regulate how consent must be obtained from consumers before using cookies and trackers and address some consent-related dark patterns (Graßl et al., 2021[95]) (negotiations regarding the proposal were ongoing at the time of writing).

AI-based dark patterns using subliminal techniques or exploiting vulnerabilities

The EC in 2021 proposed an EU regulation on artificial intelligence (EC, 2021[162]), which would, inter alia, prohibit AI systems that either deploy subliminal techniques or exploit vulnerabilities related to age, physical or mental disability in order to materially distort consumer behaviour such that it causes physical or psychological harm. Commentators consider it would thus in effect prohibit dark patterns involving AI systems of that kind (MacCarthy and Propp, 2021[163]).

Infinite scroll, autoplay, false hierarchy and preselection on social media

In the US, Senator Josh Hawley introduced to Congress in 2019 the Social Media Addiction Reduction Technology Act. On social media platforms, the bill would ban infinite scroll, autoplay, and other addictive features; require choice parity for consent, including by mandating "accept" and "decline" boxes to be designed using the same formats, fonts, and sizes; ban preselected options; provide the FTC with authority to ban other similar practices, and give consumers tools to monitor and control their use time on social media.[42] The legislation had not passed at the time of writing.

Confirmshaming

While the 2022 EC study suggests confirmshaming could be addressed by existing prohibitions in the UCPD (EC, 2022[29]), BEUC (2022[141]) proposed that the use of language and emotion to steer or guilt users into or away from making a specific choice or action (which would include confirmshaming) be specifically banned as part of the UCPD's blacklist in Annex I.

Fostering consumer-friendly digital choice architecture

In the same vein as the proposals for "fairness by design" for platforms, requirements regarding consumer-friendly digital choice architecture have been proposed for online businesses in general and can be a complement to prohibitions. They could be in the form of requirements for digital choice architecture either to be objectively neutral or to reflect what has been termed "bright" or "light" patterns (King and Stephan, 2021[149]; Graßl et al., 2021[95]), i.e. nudges steering consumers toward choices that are likely to be in their best interests, rather than those of the business.

"Bright patterns" are likely to be useful in online consumer decision-making situations where different options might be of interest to different consumers, but a particular option is clearly favoured by most. Specifically, the design might involve making it easier to make a clearly consumer welfare-enhancing choice or harder to make a clearly consumer welfare-reducing choice. They have been particularly put forward in the privacy domain (Acquisti et al., 2017[69]; Graßl et al., 2021[95]) and are reflected in the concept of "consumertarian" default rules developed by Strahilevitz and Luguri (2019[164]), i.e. requirements for settings to by default reflect the preferences or expectations of a majority of consumers. They are inherently different from disclosure and transparency measures, as they relate to the business' design of the choice architecture and the consumer decision-making process rather than the provision of information to the consumer. Hence they may reduce the burden on consumers to engage with information to ensure good consumer outcomes (see further discussion on limitations of disclosure and transparency measures below).

Such approaches could take inspiration from the GDPR's requirements for data protection to be "by design and by default" (Art. 25). A study commissioned by the German Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection (BMUV) developed a number of requirements for a consent management system to be consumer-friendly and GDPR-compliant, with a focus on privacy by default (ConPolicy, 2020[165]). BEUC (2022[141]) suggested that a general principle of "fairness by design" be incorporated into EU consumer law as part of the UCPD, to mirror the GDPR's "by design and by default" requirements.

Examples of consumer-friendly choice architecture include user interface designs that make it as easy or easier for the consumer to:

- select privacy-friendly options than it is to select privacy-intrusive options, for example by requiring the privacy-friendly option to be the default, to be more visually prominent, or to entail fewer mouse clicks or screens to navigate (e.g. a one-click "Reject all cookies" button in a cookie consent notice).
- cancel a service as it is to sign up, for example through an easily accessible one-click button (as discussed above).

Chugh and Jain (2021[134]) suggest that regulators develop guidelines for or mandate specific consumer-friendly user interfaces. In this respect, draft regulations released in 2022 by the CPPA for the CPRA, which were subject to public comment at the time of writing, would require businesses to design user interface methods for obtaining consumer consent respecting the principles "easy to understand", "symmetry in choice", "avoid language or interactive elements that are confusing to the consumer", "avoid manipulative language or choice architecture", and "easy to execute".[43]

Sometimes consumer preferences around certain choices might not be known, such as with infrequent major financial decisions, or might not clearly side with a particular option, e.g. regarding the infinite scroll practice (as discussed in Section 2). Some commentators have warned of possible adverse effects of mandating design requirements in such cases, e.g. where they lead to certain designs being promoted over others that may provide benefits to some consumers (Hurwitz, 2020[61]; NAI, 2021[166]). In such cases, interface design that requires consumers to make an active choice, without defaults, prompts or ordering options in a particular way may be optimal (CMA, 2022[167]). For example, consumers could be given an active, deliberate choice to continue viewing content on a social media platform (Nguyen and McNealy, 2021[168]). As with other remedies, experimental testing and other safeguards may be needed to ensure that the proposed consumer-friendly choice architecture is optimal (see e.g. SERNAC (2022[106]) and Graßl et al (2021[94]) for examples of testing "bright patterns").

Issuing regulatory guidance

In addition to their enforcement actions, some consumer and data protection authorities have developed guidance to business on the interpretation of relevant laws in relation to dark patterns, potentially including good practice examples, and have conducted campaigns to raise awareness with business. Examples include guidance from: the EC and the ACM concerning EU consumer law (ACM, 2020[20]; EC, 2021[141]); the European Data Protection Board (EDPB) and a number of European data protection authorities concerning EU data protection laws on obtaining consent (CNIL, 2020[161]; CNIL, 2020[169]; EDPB, 2020[170]; DSK, 2021[171]); as discussed above, the US FTC on how it applies the law to negative option marketing practices (US FTC, 2021[159]);[44] the Israel Consumer Protection and Fair Trade Authority (ICPFTA) on the use of default options that the consumer must opt out of (ICPFTA, 2022[172]); or the UK Information Commissioner's Office (ICO) regarding privacy-intrusive designs directed at children (ICO, 2020[173]). Such guidance comes on top of existing guidance specific to certain practices that have long been recognised by consumer authorities – e.g. subscription traps, drip pricing, fake testimonials – as documented in OECD (2019[3]; 2019[4]; 2019[2]). In some cases older guidance may be revised to account for certain dark patterns; for example, in 2022 the US FTC sought public comment on revisions to existing guidance on digital advertising, including to better address dark patterns.[45]

Guidance could also include visual examples of good and bad user interface designs, potentially developed in co-operation with key stakeholders such as online businesses and their trade associations, user interface designers, and consumer organisations. The CNIL, for example, has developed practical examples of interfaces aimed at helping designers comply with the GDPR (CNIL, n.d.[174]). Similarly, the EDPB released guidelines offering practical recommendations and best practices to designers and users of social media platforms on how to assess and avoid dark patterns in social media interfaces that infringe GDPR requirements (EDPB, 2022[175]). At the time of writing, the BMUV was also developing good practice examples for user-friendly and GDPR compliant cookie-banners in the framework of a project with different European stakeholders (see Section 6). Such guidance may also encourage businesses to test that their user interfaces are compliant and lead to good consumer outcomes (see Section 6 for further discussion).

Empowering regulatory authorities to take action on dark patterns

As new dark patterns may emerge quickly or existing ones tweaked slightly to evade laws, in several jurisdictions measures have been implemented or proposed to empower regulatory authorities to more readily address them. Such powers may involve the ability to make rules that prohibit or restrict specific dark patterns or to directly impose fines on businesses for their use. For example:

- In 2021, the US FTC highlighted the importance of addressing dark patterns, including by approving new compulsory process resolutions in a number of key enforcement areas, such as deceptive and manipulative conduct on the Internet relating to manipulation of user interfaces. These process resolutions were designed to enable speedier investigations of conduct in these areas.[46] The DETOUR Act, although still in the earliest legislative stages, would also have the US FTC create rules governing informed consent, independent review boards and professional standards bodies.[47]
- In 2022, the UK government agreed to give the CMA the power to enforce consumer law directly and impose directions and monetary penalties on businesses

without having to go through the civil courts,[48] having noted that the CMA's enforcement action over several years against dark patterns used by ticket resellers would have been quicker had it had such powers (UK BEIS, 2021[150]).

- In 2022, the ACCC suggested that legislation could provide it or another authority with powers to develop and implement rules governing digital platforms or services to achieve overarching objectives or principles contained in the legislation (ACCC, 2022[151]).
- As mentioned in Section 2, the definition of dark pattern adopted in the CCPA empowers the CPPA to further define by regulation what practices constitute a dark pattern (CPRA/ Cal. Civ. Code § 1798.140(l)).

Researchers have similarly proposed that consumer authorities be empowered to make relevant regulations to address dark patterns, subject to appropriate safeguards (Stigler Committee, 2019[49]; Chugh and Jain, 2021[134]). Some consumer advocates suggest consumer authorities could be given a power similar to that possessed by some securities regulators to ban harmful financial products (CPRC, 2020[148]). Furthermore, Willis (2020[39]) suggests that absent new legislation, consumer authorities and courts may also interpret existing general prohibitions in consumer law, e.g. in relation to unfair or deceptive practices, in new ways which, while still conforming to the spirit of the existing law, would allow dark patterns to be effectively addressed.

Addressing consumer vulnerability to dark patterns

Researchers and legislators in several jurisdictions have proposed prohibitions on online platforms and other online businesses from using digital practices, including those involving choice architecture, that discriminate or otherwise harm consumers of specific groups, including those that may be particularly vulnerable to certain practices (Costa and Halpern, 2019[152]; Fletcher et al., 2021[139]). Some researchers have furthermore proposed anchoring the notion of digital vulnerability, understood as a universal condition potentially applying to all consumers in the digital marketplace, in consumer law (Helberger et al., 2021[139]).

Measures to address consumer vulnerability in the digital age are further explored in the CCP's report on the topic (OECD, forthcoming[10]).

Additional considerations

Limitations of disclosure and transparency measures

In some cases, increasing transparency and using well-designed information disclosures can improve consumer outcomes online (OECD, 2018[5]; Veltri et al., 2020[175]; OECD, forthcoming[35]). However there is an abundance of evidence showing that the effectiveness of certain kinds of disclosures is mixed and strongly dependent on their design, and that in some contexts disclosure requirements may even backfire and harm consumers (AFM & ASIC, 2019[176]; Bar-Gill, Schkade and Sunstein, 2019[177]; Seizov, Wulf and Luzak, 2019[178]; Persson, 2018[179]; ACM, 2021[180]; CMA, 2022[31]; OECD, forthcoming[35]). The wide prevalence of dark patterns on cookie consent notices, as noted in Section 3, illustrates this point. Consumer advocacy groups have in particular argued that, in contrast to a "privacy by design" approach, reliance on disclosure and transparency measures may place too great a burden on the consumer to make privacy choices in their best interests (Consumer Reports Digital Lab, 2021[182]).

A number of behavioural experiments have demonstrated the limited effectiveness of information disclosure as a remedy specifically to dark patterns, for example:

- The 2022 EC study found that two measures – a "cooling-off" measure prompting the consumer to review details about their chosen product and an additional disclosure indicating they were subject to a personalised dark pattern if that were the case – had no statistically significant reduction in the effectiveness of the dark patterns tested (EC, 2022[29]).
- SERNAC found that, when consumers were prompted to accept cookies that were non-essential to the use of a webpage, providing information to them about the cookies had no statistically significant impact on their likelihood of rejecting the cookies (SERNAC, 2022[106]).
- In a drip pricing context, the ACM found that consumers almost never clicked on two kinds of clickable links providing information about the additional non-optional costs (an "i" symbol next to the price and text such as "excluding booking fees") (ACM, 2021[181]).
- The 2020 EC study found that in most cases information provision measures did not lead to a statistically significant reduction in the effectiveness of dark patterns on travel booking websites and apps (EC, 2020[101]).

Other recent experiments have also demonstrated the limited effectiveness of disclosures in relation to personalised pricing or sponsored ranking (OECD, 2021[183]; ACM, 2021[181]). On the whole, this evidence confirms that disclosure and transparency measures are not sufficient in isolation to protect consumers from dark patterns and that, if employed, their design should be carefully considered taking into account the available empirical evidence. As the CMA notes, when there is substantial evidence of harm, banning or restricting practices may be more effective (CMA, 2022[31]).

Combining principle- and rule-based regulation

Dark patterns are likely to continue to evolve and become more effective, thanks to frequent A/B testing, potentially combined with algorithmic marketing. This evolving nature favours a mix of a principle- and a rule-based approach to consumer law. Specifically, well-designed rule-based regulation, or bright-line rules, banning specific practices may help address certain dark patterns that are already in existence and considered harmful, as well as provide clarity to consumer authorities on when to intervene and businesses certainty in relation to specific designs (OECD, 2021[9]; Chugh and Jain, 2021[135]). But new dark patterns may not fit neatly into the scope of specific bans (OECD, 2021[9]; Corones et al., 2016[184]). Accordingly, well-designed, broad principle-based prohibitions on deceptive, unfair or otherwise harmful commercial practices (see examples discussed above) – which could take into consideration the likely or actual effect of the practice on the consumer, as is the case in the EU's UCPD or Section 5 of the US FTC Act – can complement rule-based regulation by providing a future-proof "safety net" and flexibility for consumer authorities and courts to address dark patterns that evade specific rules (Corones et al., 2016[184]; Paterson et al., 2015[185]; EC, 2017[186]; Willis, 2020[39]). A 2017 evaluation of the UCPD found in particular that its combination of principle-based prohibitions and blacklist of specific practices was "widely considered to provide an effective framework for achieving a high level of consumer protection regarding unfair commercial practices" (EC, 2017[186]). As discussed above, new principle-based prohibitions have also been proposed in some jurisdictions in relation to practices that could be considered "unfair" or "abusive".

Adapting interpretation of existing legal standards

In some jurisdictions, such as the EU and the US, whether a practice is deemed unfair or deceptive is evaluated from the perspective of the "average" or "reasonable" consumer targeted by the practice, who, under the EU UCPD, is understood to be "reasonably informed, circumspect, and observant consumer, taking into account social, cultural and linguistic factors".[49] But some researchers have suggested courts adopt a more nuanced understanding that better reflects the consumer as a flawed decision-maker, which may help adequately challenge dark patterns (Howells, Twigg-Flesner and Wilhelmsson, 2017[66]; Cohen, 2019[187]).[50]

Furthermore, as discussed in Section 4, over time, dark patterns are likely to become more personalised due to improved data collection combined with machine learning. Establishing proof of a personalised dark pattern's deceptive character may be difficult, as the characteristics of a dark pattern presented to the affected consumer(s) may not be similarly observable by a consumer authority, especially without access to the business' experimental data. In addition, where dark patterns are the outcome of autonomous experiments, it may be challenging to determine whether they were ultimately intended to manipulate consumers, which some courts may rely on to facilitate enforcement even if not required by law (Willis, 2020[39]). Hence some researchers have suggested that to facilitate effective enforcement, the burden should lie on the business to prove that it did not cause consumer harm (Willis, 2020[39]; Helberger et al., 2021[139]; EC, 2022[29]). Moreover, in cases of personalisation at the individual level, the EC and the ACM have considered that the average consumer should be considered a single consumer – i.e. the consumer targeted by the personalised dark pattern (ACM, 2020[20]; EC, 2021[141]).[51]

Enhancing co-operation among policy areas and across borders

Dark patterns engage a range of policy areas beyond consumer policy, such as privacy, artificial intelligence and competition. Governments should seek to engage across these disciplines, including to avoid overlapping efforts, develop synergies and determine which mechanism is best suited to address specific dark patterns. Researchers have shown how in the EU, for example, regulators can be faced with a dilemma as to whether to tackle unfair data practices via consumer, data protection or competition law (Botta and Wiedemann, 2019[188]), and that a pluralistic approach mixing strengths of different regimes may best address dark patterns (Leiser, 2020[48]).

Several jurisdictions have recognised the need for closer regulatory co-operation in the digital sphere. For example, in 2020, the UK competition, consumer, data protection and communications regulators launched the Digital Regulation Cooperation Forum, to be later joined by the financial regulator, with a view to enhancing regulatory coordination in digital markets.[52] The CMA and the ICO published a joint statement in 2021 out how they intend to enhance the synergies between their policy agendas (CMA & ICO, 2021[189]).[53] Similarly, in the Netherlands in 2021 and in Australia in 2022, regulators from different policy areas announced their close co-operation on digital matters through the Digital Regulation and Cooperation Platform [54] and Digital Platform Regulators Forum[55] respectively. The CMA, ACCC and Danish Competition and Consumer Authority (DCCA) have also set up specialised units to oversee digital platform matters from competition and consumer policy angles. Similarly, the Stigler Committee (2019[49]) proposed the creation of a specialised digital authority as a subdivision of the US FTC to focus on all aspects of digital platforms, including their use of dark patterns and risks of addiction.

Cross-border co-operation on dark patterns is also critical to ensure exchange of lessons learned, develop a common approach and avoid regulatory fragmentation. In this regard, in 2022 Didier Reynders, Commissioner for Justice of the EC, and Lina Khan, Chair of the US FTC, agreed to strengthen co-operation and exchange of good practices on consumer protection, including through increased dialogue on dark patterns.[56]

Gathering evidence to support policy making and enforcement efforts

As the OECD Consumer Policy Toolkit notes, given consumer authorities' limited resources they should generally focus on issues causing the greatest amount of consumer detriment (OECD, 2010[6]). Indeed, as discussed in Section 3, dark patterns are highly prevalent, such that enforcers will likely not be able to address all instances of them. Evidence of different dark patterns' prevalence, effects on consumer decision-making and resulting personal and structural consumer detriment is thus critical to support policy and enforcement efforts.

Specifically, highly prevalent and effective/harmful dark patterns might warrant greater attention; those that are effective but rare or prevalent but ineffective may be of less cause for concern. Indeed, as noted by Luguri and Strahilevitz (2021[25]), it is possible that aggressive policing of less effective or more benign dark patterns is not cost-justified. Moreover, dark patterns that are more likely to fall through legal gaps, for example because they do not qualify as deceptive or misleading under the law, might also warrant more urgent attention from policy makers than those for which consumer authorities already have the necessary authority. Detectability of dark patterns may also be a relevant secondary criterion to consider (noting, however, that awareness is unlikely to always protect consumers, as discussed in Section 4).

Specific tools such as those reviewed in this report may be employed in this regard:

- To identify the prevalence of dark patterns (including possible third-party entities that might create them), *mystery shopping* or *sweeping* (similar to e.g. the 2022 EC study (EC, 2022[29]) or SERNAC (2021[72])) including with manual or automated screenshot tools, *selective audits of user interfaces* (Chugh and Jain, 2021[135]; Luguri and Strahilevitz, 2021[25]) and machine learning-based *web crawling tools* (similar to e.g. by Mathur et al. (2019[24])) can be employed. In some cases, this may mean developing the necessary in-house expertise or collaborating with researchers who have developed or can develop such tools, possibly in an open-source manner (OECD, 2021[1]; Rosca et al., 2021[190]).[57] Web-crawling may also have the advantage of avoiding potential biases from relying on consumer complaints or self-reported awareness (CMA, 2022[31]).
- To assess the effectiveness of, detectability of, and detriment resulting from dark patterns, as well as the effectiveness of potential remedies, *behavioural experiments* (including laboratory experiments and online field experiments) and *consumer surveys* can be employed (similar to e.g. Luguri and Strahilevitz (2021[25]), Di Geronimo et al. (2020[73]), Graßl et al. (2021[94]), SERNAC (2022[106]) or DITP & DGCCRF (2021[110])). Regulators may also seek to obtain from businesses appearing to use dark patterns *internal marketing material, results of experiments (A/B testing)* or *coding for algorithms* for analysis by digital forensics teams and outside experts (OECD, 2021[9]; Klein, 2021[191]; Calo, 2014[18]). The CMA and ACCC, for example, leveraged information obtained from online hotel booking sites for investigations into their use of dark patterns (CMA, 2017[192]).[58] Such data and information may be critical to measuring longer term and wider impacts of dark patterns, including detriment (CMA, 2022[31]).
- To assess the extent to which existing regulatory frameworks adequately address dark patterns, particularly when found to be harmful, *legal analysis,* including review of case law and comparisons with regulatory frameworks in other jurisdictions where appropriate, can be employed (see e.g. Luguri and Strahilevitz (2021[25]) and the 2022 EC study (EC, 2022[29])).

The use of some of these tools may be subject to having relevant investigative powers. In this regard, the CCP's Implementation Toolkit on Legislative Actions for Consumer Protection Enforcement Co-operation suggests that countries should provide their consumer authorities with powers to, inter alia: require or compel the production of relevant information, subject to relevant privileges; seek to preserve evidence until it can be examined; carry out undercover investigations and covertly observe the conduct of business; and inspect or search business premises and seize potential evidence (OECD, 2021[193]).

Such evidence can help determine which dark patterns policy makers and enforcers should focus on in the first instance, but also what kind of measures may be needed (including whether e.g. new rules, better or additional enforcement, or no action may be needed). It can also help resolve specific enforcement cases. Indeed, particularly in cases where a dark pattern does not clearly contravene the law, e.g. because it does not contain obviously deceptive text and instead uses subtle design elements, evidence (whether provided by the enforcement authority or the business in question) of its effects on consumer behaviour may help determine whether a dark pattern is sufficiently problematic and actionable under law (Rimm, 2021[194]; BEUC, 2022[142]; Willis, 2020[39]). In such cases, Mathur, Mayer and Kshirsagar (2021[53]) and Willis (2020[39]) suggest that established thresholds in regulation or standards, e.g. regarding the proportion of consumers that would need to be negatively affected by a deceptive advertisement for it to be considered problematic, or new thresholds, could be applied to determine the appropriate enforcement measure. In this regard, Klein (2021[190]) suggests that comparator-based analyses commonly used in the context of assessing antitrust damages could also be applied to dark patterns.

Using existing evidence to prioritise policy and enforcement efforts

Considering evidence of detriment and of the extent to which existing regulatory frameworks address dark patterns is still emerging, it is difficult to draw definitive conclusions on how to prioritise policy and enforcement efforts at this stage. Nonetheless, evidence reviewed in this report provides some initial directions as to what those priorities might be (noting that they may change as more evidence comes to light). Specifically, policy and enforcement responses may wish to focus on:

- *Dark patterns on apps and mobile devices*. Dark patterns appear more effective on mobile screens at influencing consumer decision-making (Strahilevitz, 2021[96]; Utz et al., 2019[78]) and some evidence indicates that they are more prevalent on apps and mobile versions of services than desktop versions (Gunawan et al., 2021[75]).
- *Instances of combined or layered dark patterns.* Dark patterns appear to have a cumulative power in influencing consumer decision-making (Luguri and Strahilevitz, 2021[25]).
- *Dark patterns on major online platforms and popular websites and apps.* Popular e-commerce websites, including online marketplaces, and apps tend to feature more dark patterns (Mathur et al., 2019[24]; Gunawan et al., 2021[75]) and several dark patterns have been identified on major online platforms (Forbrukerrådet, 2018[27]; Forbrukerrådet, 2018[84]; CMA, 2020[86]).
- *Third-party entities that enable the creation of dark patterns.* Such entities are likely to be clearly in breach of consumer law to the extent they facilitate deceptive practices (see examples in Section 3) and addressing them may help stem the flow of new dark patterns (Mathur et al., 2019[24]).
- *Protecting more vulnerable consumers.* Certain subsets of consumers, who are less educated (Bongard-Blanchy et al., 2021[33]; Luguri and Strahilevitz, 2021[25]), of young age (children) (Meyer et al., 2019[137]) or under time pressure (EC, 2022[29]), have been found to be more vulnerable to dark patterns.
- *Fostering consumer-friendly digital choice architecture (e.g. "bright patterns").* User interfaces designed to nudge consumers to make choices in their best interests have been shown to work well (Graßl et al., 2021[94]; SERNAC, 2022[106]).

Furthermore, evidence reviewed in this report regarding prevalence, effectiveness, detectability, consumer detriment and possible legal gaps relating to individual dark patterns commonly identified in the literature, presented in Sections 3 and 4 and further documented in Annexes C, D and E, may also provide initial directions as to those potentially requiring greater focus, as indicated below. It should however be noted that the proper focus may depend on the sector or setting in question; as identified e.g. by the 2022 EC study (EC, 2022[29]), some dark patterns are more prevalent in certain sectors than others.

Research demonstrates that the *hard to cancel/opt out, hidden information, false hierarchy* and *preselection* dark patterns are highly prevalent in a range of areas – on e-commerce websites and apps (Di Geronimo et al., 2020[73]; EC, 2022[29]; Gunawan et al., 2021[74]), cookie consent notices (Nouwens et al., 2020[79]; Utz et al., 2019[77]; Matte, Bielova and Santos, 2020[78]; Soe et al., 2020[80]), major online platforms (ACCC, 2019[84]; CMA, 2020[85]; Forbrukerrådet, 2018[27]; Forbrukerrådet, 2018[83]; Forbrukerrådet, 2021[86]) and search engines (ACCC, 2021[88]) – are effective in influencing consumer decision-making (Luguri and Strahilevitz, 2021[25]; Utz et al., 2019[78]; Machuletz and Böhme, 2019[94]; Nouwens et al., 2020[80]; EC, 2022[29]) (see also CMA (2022[31]) regarding the power of defaults), and are relatively difficult to detect (Bongard-Blanchy et al., 2021[33]; Bhoot, Shinde and Mishra, 2020[104]), such that they may warrant greater attention.

Evidence of the relatively high prevalence on e-commerce websites and apps of *disguised ads*, *nagging* and dark patterns relating to *forced action* (including forced registration, forced disclosure) was also identified (SERNAC, 2021[72]; EC, 2022[29]; Di Geronimo et al., 2020[73]; Gunawan et al., 2021[74]; Meyer et al., 2019[136]). Though somewhat less evidence was identified pointing to their effectiveness or resulting detriment (see e.g. Luguri and Strahilevitz (2021[25]) regarding nagging and the 2022 EC study (EC, 2022[29]) regarding psychological detriment of forced action) and to the difficulty in their detection (see e.g. Bongard-Blanchy et al (2021[33]) regarding forced disclosure and a 2018 EC study regarding native advertising (EC, 2018[92])).

Dark patterns relating to urgency/scarcity (e.g. *low-stock messages* or *countdown timers*) and social proof (*activity messages* or *testimonials*) appear relatively more prevalent on e-commerce websites compared to other dark patterns (Mathur et al., 2019[24]; SERNAC, 2021[72]; Moser, Schoenebeck and Resnick, 2019[75]). But while scarcity cues tend to elicit strong negative emotions (Kristofferson et al., 2017[122]), evidence of their effectiveness is mixed, relative to social proof (Luguri and Strahilevitz, 2021[25]; EC, 2020[99]; Jeong and Kwon, 2012[100]) and they may be relatively easily detectable (Bongard-Blanchy et al., 2021[33]). Accordingly, while the high prevalence of scarcity cues suggest consumer authorities should continue to monitor them, they may be a lower priority relative to social proof and other dark patterns. Moreover, as discussed in Section 2, where social proof and urgency dark patterns are truthful, they may not be considered deceptive and at times be beneficial to some consumers.

Other dark patterns also present disparities in the available evidence reviewed on their prevalence and effectiveness/detriment. Specifically, there is evidence of the effectiveness of or financial detriment resulting from *hidden costs / drip pricing* (see e.g. Blake et al. (2021[109]) and CMA (2022[31])), *hidden subscriptions/forced continuity* (see e.g. ECC Sweden (2017[69]) and a 2016 EC study (EC, 2016[71])), *trick questions* (Luguri and Strahilevitz, 2021[25]) and *friend spam/social pyramid*.[59] However some evidence suggests they are relatively less prevalent on e-commerce websites and apps than other dark patterns (Mathur et al., 2019[24]; SERNAC, 2021[72]; EC, 2022[29]; Gunawan et al., 2021[74]), and that forced continuity is relatively more straightforward for consumers to detect (Bhoot, Shinde and Mishra, 2020[104]).[60] *Confirmshaming* appears common on major online platforms (Forbrukerrådet, 2018[27]; CMA, 2020[86]), but less common on e-commerce websites and apps in general (EC, 2022[29]). It also presents mixed evidence regarding its effectiveness (Luguri and Strahilevitz, 2021[25]; EC, 2022[29]) and has been found to be relatively easy to detect (Bhoot, Shinde and Mishra, 2020[104]; Bongard-Blanchy et al., 2021[33]). Moreover, for the *gamification*, *price comparison prevention*, *intermediate currency, sneak into basket, bait and switch, immortal accounts, infinite scroll* and *autoplay* dark patterns, evidence regarding prevalence points either to low prevalence on e-commerce websites and apps in general and cookie consent notices (see Annex C for further details) or it was not available. And while there is evidence of the detectability of some of such dark patterns, evidence appears insufficient regarding their effectiveness and resulting detriment.

Finally, as discussed above, there may also be other disparities between dark patterns in terms of coverage by existing regulatory frameworks, which could further determine policy priorities. For instance, according to Temby and Vasquez (2020[146]), hard to cancel may not meet the bar of a misleading and deceptive act in Australian consumer law, and according to Hung (2021[56]), nagging may not meet the bar of a deceptive or unfair act in consumer law in the US.

Overall, where dark patterns exhibit disparities in evidence regarding their prevalence, effectiveness/detriment and possible legal gaps, consumer and data protection authorities and policy makers should be alert for them while seeking to gather further evidence to determine and refine measures and priorities. Additionally, as discussed in Section 4, depending on the dark pattern, detriment at the individual consumer level may be exacerbated by detriment collectively, e.g. in terms of competition impacts. For instance, this may be the case for drip pricing, certain privacy-intrusive dark patterns (e.g. pre-selection), addictive dark patterns and obstruction-related dark patterns (e.g. price comparison prevention, hard to cancel). Policy makers and enforcers might therefore optimally focus their efforts on those dark patterns found to cause detriment across multiple dimensions, in terms of both personal and structural detriment.

6. Educational, technical and business initiatives to address dark commercial patterns

Key points

- Several measures exist to educate consumers about dark patterns, including information campaigns from consumer authorities and tools to report, raise awareness about or shame businesses for dark patterns currently in use.
- Technical tools have been or are being developed to help consumers mitigate or remove dark patterns, such as browser extensions and apps and other software.
- Various self- and co-regulatory initiatives have relevance to addressing dark patterns, for example through principle-based standards governing interactions with consumers online, and some national advertising self-regulatory bodies have taken action to address various dark patterns.
- Calls among the user interface design community to raise awareness about dark patterns and adopt ethical design standards have increased in recent years, with some designers developing ethical design guidelines and toolkits.
- Some commentators have proposed mechanisms for online businesses to review their choice architecture to identify dark patterns, including self-auditing and using experiments to test compliance.
- While consumer education and technical measures and self- or co-regulatory initiatives can play an important supporting role in protecting consumers from dark patterns, they are insufficient in isolation and should be seen as complementary to robust regulatory and enforcement measures.

Educational measures and technical consumer tools to address dark patterns

Raising awareness and educating consumers about dark patterns

A number of consumer authorities have conducted information campaigns to raise awareness about and help consumers avoid dark patterns, including the Mexican consumer protection authority (PROFECO), SERNAC, the CMA and the Peruvian consumer protection authority (Indecopi) (PROFECO, 2020[196]; SERNAC, 2021[72]).[61] Researchers have also proposed that, in some circumstances, educational interventions that seek to build cognitive competencies in consumers and their ability to control their online environment (known as "boosting") so that they can more effectively protect themselves from dark patterns may help, e.g. encouraging adoption of certain procedural rules before making a choice (Kozyreva, Lewandowsky and Hertwig, 2020[197]; Graßl et al., 2021[94]; Bongard-Blanchy et al., 2021[33]). In this context, some evidence shows that targeted interventions to raise consumers' awareness of dark patterns and develop their "manipulation literacy" or "critical digital literacy" may help them identify and avoid dark patterns (Magnusson, 2019[198]; DITP & DGCCRF, 2021[110]; Bell and Fitton, 2021[137]; Di Geronimo et al., 2020[73]).

Several tools have been developed or proposed to report, raise awareness about or shame businesses for dark patterns in use. For example, darkpatterns.org provides a "hall of shame" and runs a twitter feed providing examples of significant recent dark patterns.[62] Similarly, darkpatterns.uxp2.com provides a corpus of examples of dark patterns identified by user experience (UX) practitioners. The Dark Patterns Tip Line, the Dark Pattern Detection Project and a dedicated Reddit thread provide an avenue for consumers to report and see examples of dark patterns.[63] Costa and Halpern (2019[151]) propose that consumer groups establish an annual, consumer-led “sludge award” for the online business found to employ the most sludge, so as to incentivise such businesses to change their practices.

Browser, app and software tools to detect, mitigate or remove dark patterns

Several researchers have proposed or developed browser tools consumers can use to detect or mitigate dark patterns on websites, particularly in relation to privacy. Matte, Bielova and Santos (2020[78]) developed a browser extension, “Cookie glasses”, enabling consumers to determine if consent stored by CMPs corresponds to their choice. Global Privacy Control consists of a browser setting or extension allowing consumers to notify businesses’ websites of their privacy preferences.[64] The Consent-O-Matic extension automatically answers consent notices for the consumer after having set cookie preferences once, so as to mitigate risks of manipulation by specific consent notices;[65] similarly, Advanced Data Protection Control is a proposed mechanism for automated communication of consumers’ privacy decisions in a browser, plugin or operating system.[66] Mathur et al. (2019[24]) propose the development of a browser extension to automatically detect dark patterns based on their dataset, which could be augmented with further dark patterns over time.

Researchers and businesses have sought to build software tools for consumers to address dark patterns selectively. Truebill, for example, aims to assist consumers in identifying and cancelling unwanted subscriptions.[67] AppGenie (formerly “GreaseDroid”) aims to be a community-driven app modification framework enabling consumers to disable dark patterns in apps selectively (Kollnig, Datta and Van Kleek, 2021[199]). Similarly, the Dark Pattern Detection Project aims to build a "Dark Pattern Detection App" that uses AI-based text analysis to automatically recognise dark patterns, which the consumer can then redesign.[68] However, while some dark patterns are amenable to automated identification using text, images or HTML code, others may require manual verification or may not be detectable at all via webcrawling due to variation in how the pattern is defined or implemented (Stavrakakis et al., 2021[77]). An example is the hard to cancel dark pattern, which may not be detectable at the time of signing up to the subscription (Hausner and Gertz, 2021[200]).

Business initiatives and tools to address dark patterns

Existing self- and co-regulatory initiatives relevant for dark patterns

Several advertising and marketing self- or co-regulatory initiatives in various jurisdictions address dark patterns, in that they include principles relating to online advertising, some aspects of user interface design and other online commercial practices.

For example, the International Chamber of Commerce’s (ICC) Advertising and Marketing Communications Code contains principles encouraging marketers to be honest and truthful and not mislead; to not abuse the consumer’s trust or exploit their lack of knowledge; to communicate factors likely to affect consumers’ decisions such that they can be taken into account; to use genuine testimonials; to identify advertising as such; and protect consumer privacy when collecting personal data (ICC, 2018[201]). According to the ICC, self-regulatory bodies in 42 countries have developed or are developing national codes based on its code.

At the national and regional level, self-regulatory principles of the Network Advertising Initiative (NAI) or Digital Advertising Alliance in the US, or the European Digital Advertising Alliance, for example, require businesses to, inter alia, adopt clear information disclosures regarding use of consumer data and transparent mechanisms for consumers to exercise choice regarding their data.[69] The NAI has also developed best practices regarding user choice and transparency to assist businesses in avoiding dark patterns involving collection of consumer data (NAI, 2022[202]). The Code of Non-broadcast Advertising and Direct & Promotional Marketing (CAP Code) of the Advertising Standards Authority, a self-regulatory body for the advertising industry in the UK, contains principles addressing certain dark patterns such as drip pricing, disguised advertisements and subscription traps.[70] Moreover, the BBB National Programs' National Advertising Division (NAD) and Children's Advertising Review Unit (CARU), self-regulatory bodies in the US for advertising and children's advertising respectively, seek to hold businesses to the FTC's advertising standards, including by providing recommendations to cease use of dark patterns following a claim made by a competing business and referring matters to the FTC for enforcement action (Brett, 2021[203]). The French advertising self-regulatory body (ARPP), has applied an AI-based tool to detect breaches of its advertising code, including use of fake countdown timers.[71] These and other national advertising self-regulatory bodies have taken actions to address various dark patterns, such as limited stock messages, drip pricing, disguised ads, forced disclosure, hidden information and countdown timers, on the basis of a breach of a national code or guidelines.[72]

In 2018 the BMUV launched its Corporate Digital Responsibility (CDR) initiative, which encourages businesses to take on greater responsibilities in the digital sphere going beyond legal requirements. The initiative is supported by the CDR Code, containing principles that companies that have signed up to the initiative agree to adhere to, including to avoid consumer harm and discrimination, be transparent and accountable, and respect consumer autonomy (BMUV, 2021[204]). Within the framework of the CDR initiative, the BMUV launched a project to develop examples for consumer-friendly cookie banners together with different European stakeholders from the private sector, civil society and public sector. France's Plateforme RSE, a multi-stakeholder consultation body reporting to the French prime minister on corporate social responsibility issues, has similarly advanced the CDR concept and made recommendations to further its uptake, including through greater regard for ethical use of digital technology (Plateforme RSE, 2020[205]).

Emerging business initiatives and tools

Calls among the UI/UX (user interface/user experience) design community to raise awareness about dark patterns, hold businesses accountable through public shaming and adopt ethical design standards and best practices have increased in recent years (Fansher, Chivukula and Gray, 2018[206]; Chivukula et al., 2020[207]; Shaw, 2019[120]). Designers have in particular suggested that there be an ethical code of practice or formal standards for the UI/UX community to abide by (Bunker, 2013[208]; Beattie, Lacey and Caudwell, 2020[46]; Shamonsky, 2018[209]) and greater ethics education in UX design courses (Gray, Chivukula and Lee, 2020[210]; Beattie, Lacey and Caudwell, 2020[46]). Existing examples of codes of conduct or ethics applicable to UI/UX design include the User Experience Professionals Association Code of Professional Conduct [73] and the Design Institute of Australia Code of Ethics[74]. The proposed US DETOUR Act suggested the creation of a professional standards body focusing on user design best practices for large operators.[75] Several designers have also developed their own practical guidelines, checklists or toolkits on how to avoid dark patterns and design interfaces more ethically (Falbe, Frederiksen and Andersen, 2020[211]; Meske and Amojo, 2020[212]; Zhou, 2022[213]; Institute for the Future and Omidyar Network, 2018[214]; Nielsen, 2020[215]).

Some commentators have suggested that businesses put in place mechanisms to review their choice architecture and business processes to identify and mitigate dark patterns. Sunstein (2020[215]) proposes that firms conduct "sludge audits", i.e. regular reviews of unnecessary frictions in consumer decision-making processes, and other audit tools have been proposed for businesses to self-assess their algorithms (de Marcellis-Warin et al., 2022[217]). Soman et al. (2019[218]) developed a dashboard that businesses could use to monitor, track, and correct sludge in their digital interfaces. Bongard-Blanchy et al. (2021[33]) planned to develop a standardised transparency impact assessment process for interface design. Other commentators suggest that online businesses use A/B testing and self-audits not only to test for conversion rates of a user interface but also from perspective of the consumer's best interests and compliance with the law (Van Der Lee et al., 2021[219]; Klein, 2021[191]; Luguri and Strahilevitz, 2021[25]) and to solicit user feedback to make it user-friendly (Chugh and Jain, 2021[135]).

Complementarity to robust regulatory and enforcement measures

Self- or co-regulatory initiatives such as codes of conduct and ethics can play an important supporting role in protecting consumers from dark patterns, for example where targeted policy responses are yet to be fully developed, where they provide additional protections beyond legal requirements, or where they play a monitoring and enforcement role supplementing a consumer authority (OECD, 2015[220]).

But their success depends on a number of factors (OECD, 2015[220]), and they are unlikely to be sufficient consumer protection measures in isolation. A broad review of self and co-regulatory initiatives found, for example, that where industry players have a significant steer in the design of such initiatives, this risks lower standards, undermining policy goals and regulatory capture (McEntaggart, Etienne and Uddin, 2019[221]). The Stigler Committee (2019[49]) considered that attempts for industry to self-regulate in the US to address privacy concerns were not successful due to lack of adoption, limited consumer protections and lax enforcement and monitoring. Participants at a 2021 US FTC workshop on dark patterns also found self-regulation may assist, but not replace, effective enforcement action from consumer authorities (US FTC, 2021[222]).

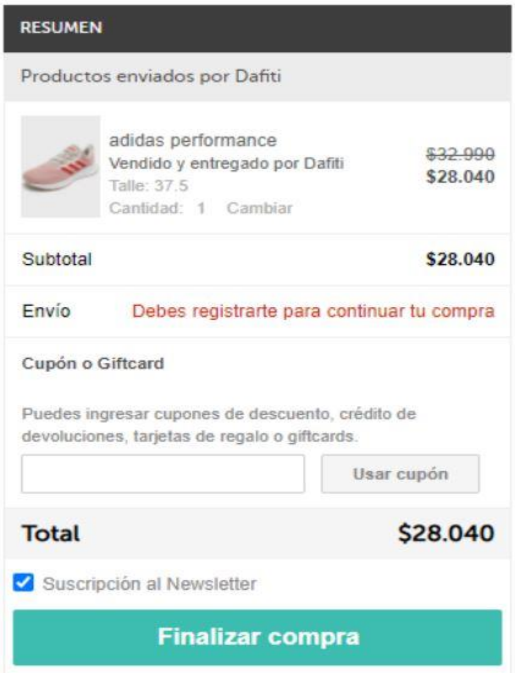
Nonetheless, as mentioned in Section 5, industry can play an important role in working with regulators and policy makers to both develop workable policy responses and establish best practices, e.g. as part of regulatory guidelines. Furthermore, as discussed in Section 4, businesses employing dark patterns can gain unfair advantages over those that do not, for example by extracting more sales, personal data or attention time than otherwise or by hindering consumers' ability to choose competing businesses. Hence businesses have competitive incentives to seek strong enforcement of rules mitigating dark patterns in order to maintain a level playing field.

In the same vein, a number of education, awareness-raising and technical consumer tools and measures can also play a supporting role in protecting consumers from dark patterns. However, the significant information asymmetries that characterise dark patterns mean that even well-informed and well-tooled consumers are generally unlikely to be on an equal footing with businesses that employ them. As discussed in Sections 4 and 5, awareness is unlikely to be sufficient to protect consumers from most dark patterns and disclosure and transparency measures are limited in their effectiveness in addressing dark patterns. In addition, the rapid evolution of dark patterns, characterised by increasing complexity and subtlety, means that such measures may often be solutions to yesterday's dark patterns. Hence such measures should also be seen as complementary to robust regulatory and enforcement measures.

Annex A. Examples of dark patterns on websites and apps

Figure A.1. Example of forced registration dark pattern

The consumer is forced to register in order to make a purchase



RESUMEN

Productos enviados por Dafiti

adidas performance
Vendido y entregado por Dafiti
Talle: 37.5
Cantidad: 1 Cambiar

~~$32.990~~
$28.040

Subtotal	$28.040
Envío	Debes registrarte para continuar tu compra

Cupón o Giftcard

Puedes ingresar cupones de descuento, crédito de devoluciones, tarjetas de regalo o giftcards.

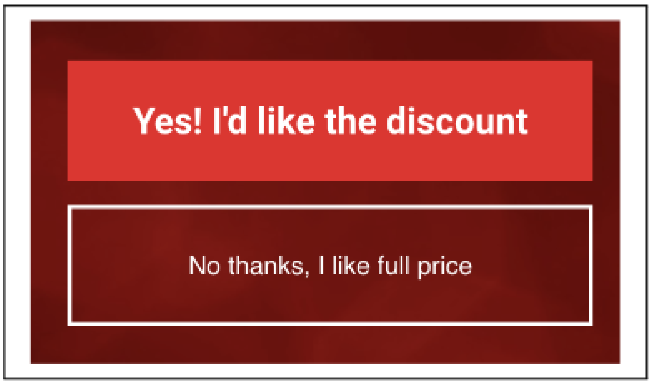
Total	$28.040

☑ Suscripción al Newsletter

Note: "Debes registrarte para continuar tu compra" translates to "You must register to continue your purchase".
Source: SERNAC (2021[72]).

Figure A.2. Example of a confirmshaming dark pattern

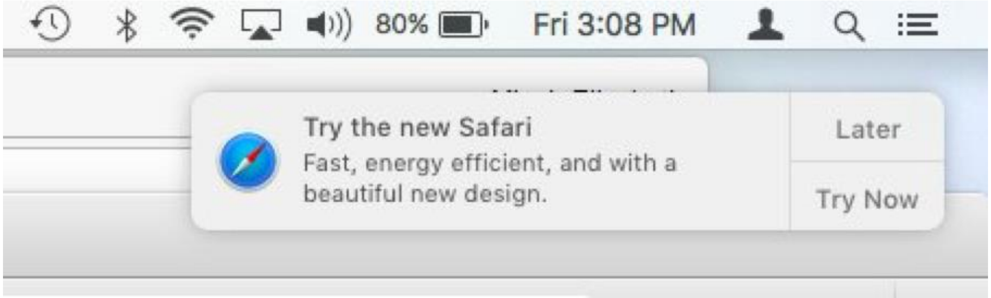
The consumer is shamed into opting for a discount.



Source: Mathur et al (2019[24]).

Figure A.3. Example of nagging dark pattern

A dialogue box that does not provide the option to permanently dismiss the message.

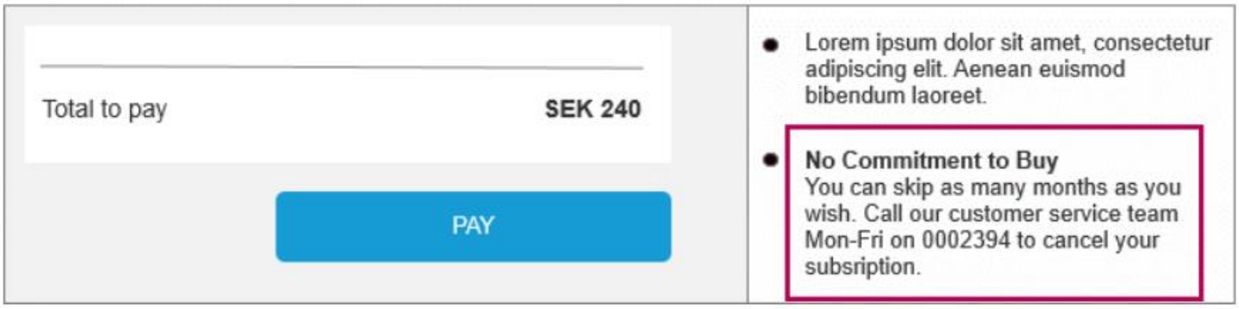


Try the new Safari
Fast, energy efficient, and with a beautiful new design.

Source: https://darkpatterns.uxp2.com/pattern/apple-no-no-option/

Figure A.4. Stylised example of hard to cancel dark pattern

The consumer is required to call to cancel their subscription.



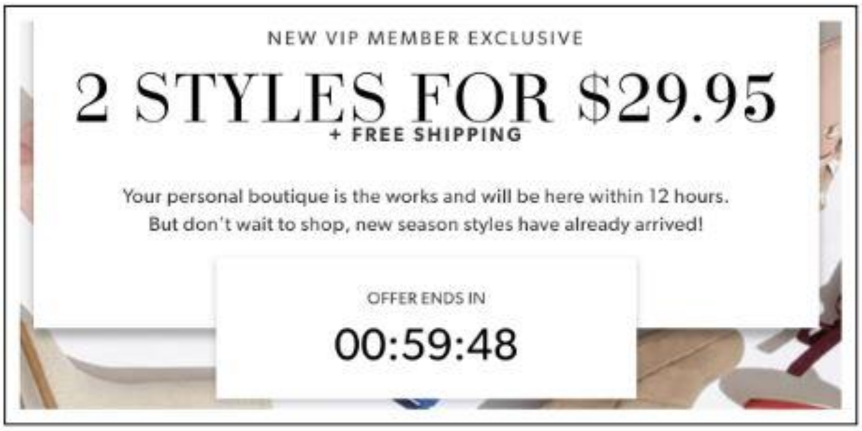
Total to pay SEK 240

- Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean euismod bibendum laoreet.
- **No Commitment to Buy**
  You can skip as many months as you wish. Call our customer service team Mon-Fri on 0002394 to cancel your subsription.

Source: Konsumentverket (2021[222]).

Figure A.5. Example of a countdown timer

A countdown timer for an offer that continues to be available even after the timer expires.



NEW VIP MEMBER EXCLUSIVE

2 STYLES FOR $29.95

+ FREE SHIPPING

Your personal boutique is the works and will be here within 12 hours.
But don't wait to shop, new season styles have already arrived!

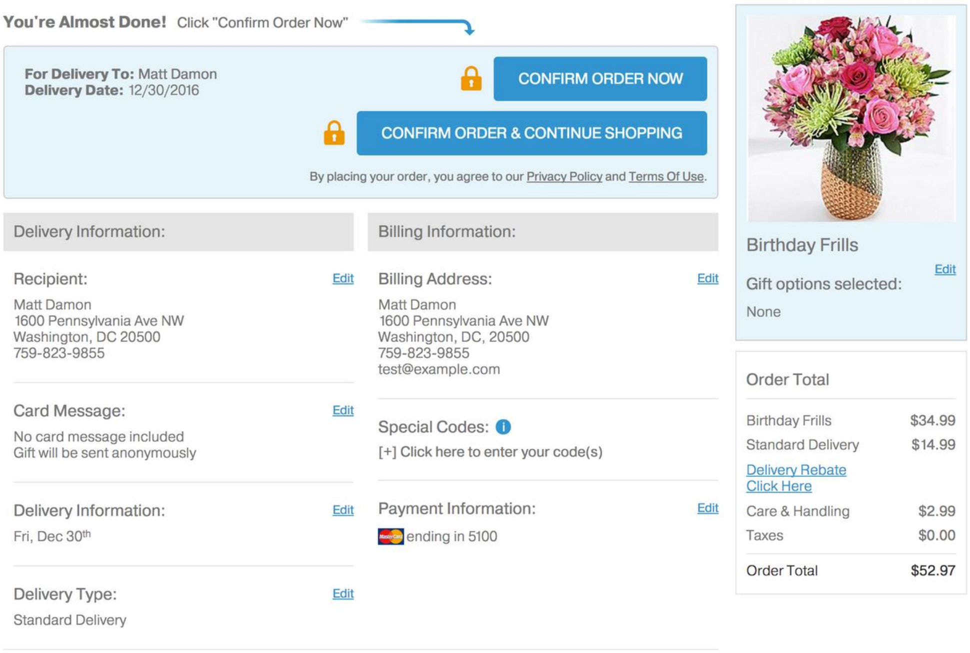
OFFER ENDS IN

00:59:48

Source: Mathur et al. (2019[24])

Figure A.6. Example of hidden costs / drip pricing

Non-optional charges are added to the total price at the final stage of the transaction



You're Almost Done! Click "Confirm Order Now"

For Delivery To: Matt Damon
Delivery Date: 12/30/2016

CONFIRM ORDER NOW

CONFIRM ORDER & CONTINUE SHOPPING

By placing your order, you agree to our Privacy Policy and Terms Of Use.

Delivery Information:

Recipient: Edit
Matt Damon
1600 Pennsylvania Ave NW
Washington, DC 20500
759-823-9855

Card Message: Edit
No card message included
Gift will be sent anonymously

Delivery Information: Edit
Fri, Dec 30th

Delivery Type: Edit
Standard Delivery

Billing Information:

Billing Address: Edit
Matt Damon
1600 Pennsylvania Ave NW
Washington, DC, 20500
759-823-9855
test@example.com

Special Codes:
[+] Click here to enter your code(s)

Payment Information: Edit
ending in 5100

Birthday Frills
Edit
Gift options selected:
None

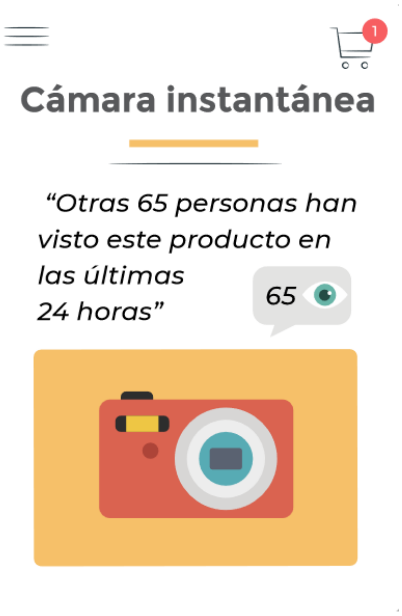
Order Total

Birthday Frills	$34.99
Standard Delivery	$14.99
Delivery Rebate Click Here	
Care & Handling	$2.99
Taxes	$0.00
Order Total	$52.97

Source: Adapted from https://www.darkpatterns.org/types-of-dark-pattern/hidden-costs

Figure A.7. Stylised example of activity notifications

Activity notifications indicating that other consumers are viewing the same product, which may be misleading or false



Cámara instantánea

"Otras 65 personas han visto este producto en las últimas 24 horas"

Note: "Otras 65 personas han visto este producto en las últimas 24 horas" translates to "65 other people have seen this product in the last 24 hours".
Source: PROFECO (2020[195]).

Annex B. Example of consolidated taxonomy of dark patterns

Category	Name of dark pattern	Description	Source
Forced action	Forced registration	Consumer forced to register or tricked into thinking registration necessary	Bösch et al. (2016[21])
	Forced disclosure / Privacy zuckering	Consumer tricked or forced into sharing more personal information than desired	Bösch et al. (2016[21]); Gray et al. (2018[23]); Brignull (n.d.[11])
	Friend spam / Social pyramid / Address book leeching	Manipulative extraction of information about other users	Bösch et al. (2016[21]); Gray et al. (2018[23]); Brignull (n.d.[11])
	Gamification	Certain aspects of a service can only be "earned" through repeated use of service	Gray et al. (2018[23])
Interface interference	Hidden information	Important information visually obscured	Gray et al. (2018[23])
	False hierarchy	Visual prominence given to firm's preferred setting or version of a product	Gray et al. (2018[23]); Mathur et al. (2019[24])
	Preselection	Firm-friendly default is preselected (e.g. more expensive or less privacy-protecting option)	Bösch et al. (2016[21]); Gray et al. (2018[23])
	Misleading reference pricing	Price shown as a discount from a misleading or false reference price	OECD (2019[3]); CMA (2022[31]); EC (2022[29])
	Trick questions	Intentional or obvious ambiguity (e.g. double negatives)	Gray et al. (2018[23]); Mathur et al. (2019[24]); Brignull (n.d.[11])
	Disguised ads	Consumer induced to click on something that isn't apparent advertisement	Gray et al. (2018[23]); Brignull (n.d.[11])
	Confirmshaming / Toying with emotion	Emotionally manipulative framing to make consumer select a particular option	Brignull (n.d.[11]); Gray et al. (2018[23]); Mathur et al. (2019[24])
Nagging	Nagging	Repeated requests to do something firm prefers	Gray et al. (2018[23])
Obstruction	Hard to cancel or opt out / Roach motel / Click fatigue / Ease	Asymmetry in ease of signing up/opting in to a product or firm-friendly choice versus cancelling/opting out	Brignull (n.d.[11]); Dapde (n.d.[26]); Gray et al. (2018[23]); Forbrukerrådet (2018[27]); Mathur et al. (2019[24])
	(Price) comparison prevention	Frustrates comparison shopping regarding price or content	Gray et al. (2018[23]); Mathur et al. (2019[24]); Brignull (n.d.[11])
	Immortal accounts	Account and consumer information cannot be deleted	Bösch et al. (2016[21])
	Intermediate currency	Purchases in virtual currency to obscure cost	Gray et al. (2018[23])
Sneaking	Sneak into basket	Item consumer did not add is in cart	Brignull (n.d.[11]); Gray et al. (2018[23]); Mathur et al. (2019[24])
	Hidden costs / Drip pricing	Costs obscured or disclosed late in transaction	Brignull (n.d.[11]); Gray et al. (2018[23]); Mathur et al. (2019[24]); OECD (2019[3])
	Hidden subscription / Forced continuity	Unanticipated or undesired automatic renewal of a service	Brignull (n.d.[11]); Gray et al. (2018[23]); Mathur et al. (2019[24])
	Bait and switch, including bait pricing	Consumer is offered product or price different from that originally advertised	Brignull (n.d.[11]); Gray et al. (2018[23]); OECD (2019[3])
Social proof	Activity messages	Indications about other consumers' actions, which may be misleading or false	Mathur et al. (2019[24])
	Testimonials	Statements from other consumers regarding a product, which may be misleading or false	Mathur et al. (2019[24])
Urgency	Low stock / High demand message	Indication of limited quantities of a product, which may be misleading or false	Mathur et al. (2019[24])
	Countdown timer / Limited time message	Indication of an expiring deal or discount, which may be misleading or false	Mathur et al. (2019[24])

Source: Consolidated taxonomy adapted from Luguri and Strahilevitz (2019[223]; 2021[25]). Sources for individual taxonomies containing each dark pattern are indicated in the table.

Annex C. Selected evidence of the prevalence of dark patterns

Area	Source	Methodology	Key findings
E-commerce websites	SERNAC (2021[72]).	Internet sweep of 107 Chilean online businesses' websites for dark patterns.	• 69 dark patterns were identified on 107 businesses' websites reviewed, i.e. on 64% of websites. • The dark patterns identified were forced action (registration) (28% of websites), urgency and scarcity cues (21%), misleading testimonials (17%), misdirection/false hierarchy (12%), sneak into basket (9%), price comparison prevention (7%), drip pricing or hidden costs (6%), hard to cancel / roach motel (2%) and forced continuity or hidden subscriptions (2%).
	Mathur et al. (2019[24]).	Web crawl of around 53 000 product pages from 11 286 popular shopping websites (understood as a website offering a product for purchase) ranked by web-traffic service Alexa, from a variety of sectors. Further examination was conducted of the top three most frequent dark patterns specifically to identify deceptive practices (i.e. where information was demonstrably false).	• 1 818 instances of dark pattern, together representing 15 types and 7 broader categories, were identified on 1 254 of the 11 286 e-commerce websites studied, i.e. roughly 11.1% of the websites. • Shopping websites that were more popular were more likely to feature dark patterns. • The dark patterns identified were: low-stock message (5.15% of websites), countdown timer (3.20%), activity message (2.34%), confirmshaming (1.45%), limited-time message (0.74%), pressured selling (0.55%), high-demand message (0.38%), hard to cancel / roach motel (0.27%), visual interference (0.21%), hidden subscription (0.12%), testimonials (0.11%), trick questions (0.08%), sneak into basket (0.06%), forced enrolment (0.05%) and hidden costs (0.04%).* • The majority of dark patterns identified was considered covert (for steering the consumer to make specific purchases without their knowledge), deceptive (for inducing false beliefs), and information hiding in nature. • Of the 361 websites containing countdown timers, 264 containing activity messages, and 581 containing low-stock messages, respectively 140 (39%), 20 (8%), and 17 (3%) were considered to feature a deceptive version of the practice. • 22 third-party entities that provide the ability to create and implement dark patterns on websites, including via plugins for online marketplaces, were identified, two of which openly advertised practices that enable deceptive messages.
	Moser, Schoenebeck and Resnick (2019[75])	Systematic content analysis involving manual screenshots of top 200 e-commerce websites in the US (referring to 186 online goods retailer sites and 14 online travel booking sites) for impulse buying features	• 75% of websites had at least 16 features that can encourage impulse buying, and 100% of websites included at least 4 features that can encourage impulse buying. • 116 (58%) of websites featured at least one instance of indication of limited-time discount; 34 (17%) of low stock warning; 29 (14%) of requiring an account to buy, 27 (13%) of a limited-time discount with countdown clock; 13 (6%) of the number sold/number of customers; 12 (6%) of limited-time product availability (no clock); 11 (5%) of the number of customers interested/watching; and 2 (1%) of limited-time product availability (with clock). *

Apps, including children's apps	Radesky et al. (2022[58])	Cross-sectional study of a sample of apps used by 160 children aged 3 to 5 years	• The majority of apps was associated with manipulative design features that included parasocial relationship pressure, fabricated time pressure, navigation constraints, and use of attractive lures to encourage longer gameplay or more purchases, in addition to advertisement-based pressure. • Only 20% of apps had no manipulative design features. • Children from lower socioeconomic strata played apps with more manipulative design.
	ACCC (2021[91]).	Analysis of consumer reviews of the top 1 000 grossing and "free" apps on the Apple App Store and Google Play Store.	• The term "subscription" featured in 44 156 negative App Store reviews and 53 594 negative Play Store reviews. • The issues raised in a sample of apps included consumers not appearing to have understood that they were agreeing to a subscription or the price of the subscription, and consumers indicating they were unable to cancel (*hidden subscription/forced continuity*)
	Di Geronimo et al. (2020[73])	Manual assessment of the 30 most trending apps from each of eight different categories of apps in the Google Play store, for a total of 240 Google Play apps. The list also included apps such as Facebook, Amazon, Twitter, Netflix, and Spotify.	• 95% of the 240 apps reviewed featured one or more dark patterns. Overall, 1 787 dark patterns were found among all apps, with an average of 7.4 dark patterns per app. 49% of the apps included 7 or more dark patterns, (N=118), 37% contained between 3 to 6 dark patterns (N=89), and only around 10% included 0, 1, or 2 dark patterns (N=33). • The dark patterns identified were: false hierarchy (61% of apps), preselection (60%), nagging (55%), hard to cancel/roach motel (41%), forced action (38%), disguised ads (33%), aesthetic manipulation (33%), forced disclosure / privacy zuckering (31%), hidden information (31%), bait and switch (16%), intermediate currency (10%), price comparison prevention (10%), toying with emotion (combines confirmshaming and countdown timers) (9%), social pyramid (6%), sneak into basket (1%) and trick questions (0%). • The high prevalence of nagging related to interruptions of the consumer, e.g. to ask permissions, rate their product or to show ads. Often such pop-ups gave one or more options to the consumer, and often the option that benefited the app was aesthetically favoured, reflecting the high prevalence of the false hierarchy dark pattern. The high frequency of the preselection dark pattern related mainly to notification preselection (push, email and SMS), with 81 apps containing more than two notifications preselected.
	Meyer et al. (2019[136])	Manual review of the prevalence of advertising in 135 children's apps, many of which were the most popular on the Google Play Store.	• 95% of the 135 apps contained at least one type of advertising, many of which were specifically designed to look part of the app.[76] These included use of commercial characters (42%); full-app teasers (46%); advertising videos interrupting play (e.g. pop-ups [35%] or to unlock play items [16%]); in-app purchases (30%); prompts to rate the app (28%) or share on social media (14%); distracting ads such as banners across the screen (17%) or hidden ads with misleading symbols such as "$" or camouflaged as gameplay items (7%). • Advertising was significantly more prevalent in free apps vs paid apps (100% vs 88%), but occurred at similar rates in apps labelled as "educational" versus other categories.

Websites and apps	EC (2022[29])	Mystery shopping of 45 popular European/national websites and 30 popular European/national apps in 16 EU countries	• 97% of the 75 websites/apps contained at least one dark pattern. • The dark patterns identified were preselection (55% of websites/apps), hidden information/false hierarchy (55%), nagging (45%), hard to cancel / roach motel (44%), forced registration (43%), disguised ad (31%), countdown timer/ limited time message (24%), toying with emotion (23%), hidden costs (17%), intermediate currency (15%), low stock / high demand message (13%), activity messages (13%), hidden subscription/forced continuity (12%), testimonials (12%), bait and switch (7%), confirmshaming (5%), price comparison prevention (5%), sneak into basket (4%), and trick questions (3%). • The most common dark patterns identified on: o online goods retailers and marketplaces websites/apps were hidden information/false hierarchy, countdown timer/limited time message, preselection and hard to cancel / roach motel. o social media and social networks were preselection, hidden information/false hierarchy, disguised ad and hard to cancel / roach motel. o arts and entertainment websites/apps were preselection, hidden information/false hierarchy and forced registration. o health and fitness websites/apps were nagging, forced registration and preselection. o transport and travel websites/apps were preselection, disguised ad, hidden information, roach motel, activity message and nagging. o gambling and games websites/apps were intermediate currency and nagging. o search engine and internet browsers were disguised ads, hidden information/false hierarchy and price comparison prevention.
	Gunawan et al (2021[74])	Manual investigation of prevalence of dark patterns on the app, mobile browser, and desktop browser modalities of 105 popular online services	• All of the services in the corpus include at least one type of dark pattern, with the majority including seven or more types. • Dark pattern usage frequently differed across the versions of a given service: quantitatively, apps tended to have more unique dark patterns than their web counterparts, and qualitatively, apps tended to include different patterns than the corresponding websites. • Popular apps included slightly more types of dark patterns overall. • Individually, of the 46 dark patterns examined, 30 appeared more frequently in the app modality. • The most prevalent dark patterns identified across desktop, mobile and app modalities were forced disclosure / privacy zuckering, forced action, preselection, hard to cancel/roach motel, nagging, aesthetic manipulation and false hierarchy. • The least prevalent dark patterns identified across desktop, mobile and app modalities were sneaking, bait and switch, hidden information, hidden costs, social pyramid, toying with emotion, trick questions, gamification and forced continuity. Slightly higher prevalence was recorded for intermediate currency and disguised ads.
	ICPEN (2019[15])	Internet sweep focused on "dark nudges" of 1760 ecommerce websites/apps in 22 ICPEN member countries in a variety of sectors.	• Of those websites/apps swept, 429 (24%) were flagged for potential "dark nudge" problematic conduct. • The three most commonly identified types of dark nudges in the sweep related to urgency (e.g. scarcity cues, countdown timers), drip pricing and "design issues" (e.g. pre-ticked boxes).
Cookie consent notices	VZBV (2021[82])	Sweep of cookie consent notices on 949 German websites from various sectors, such as travel, food delivery services or insurance	• Many of the cookie banners were found to be in a legal grey area, and about 10% were identified as clearly illegal with warnings were issued to the responsible companies. • 5.7% of websites were found to assume consent to tracking by browsing and 2.6% of websites featured pre-ticked consent *(preselection)*.

	noyb (2021[81])	Sweep of cookie consent notices on popular European websites to identify compliance with the GDPR and issue legal complaints	• Of the 560 pages where a complaint was issued: ○ 90% did not provide a way to easily withdraw consent *(hard to cancel/opt out)*. ○ 81 % did not offer a “reject” option on the initial page *(hard to cancel/opt out)*. ○ 73% used deceptive colours and contrasts to lead users to click the “accept” option *(false hierarchy)*. ○ 51% provided a link instead of a button to reject *(hard to cancel/opt out)*. ○ 15% featured pre-ticked consent boxes *(preselection)*.
	Nouwens et al. (2020[79])	Web scraping of cookie consent notices on the top 10 000 UK sites ranked by web-traffic service Alexa	• Implicit, rather than explicit, consent featured on around two thirds (32.5%) of the sites reviewed *(preselection)*. • Most consent notices made rejecting tracking substantially more difficult than accepting it, with 50.1% of sites missing a “reject all” button, and only 12.6% having one that was accessible with the same or fewer clicks as an “accept all” button *(hard to cancel/opt out)*. • When users wanted to amend specific consent settings rather than accept all, they were often faced with pre-ticked boxes of the type specifically forbidden by the GDPR: 56.2% of sites pre-ticked optional vendors or purposes/categories *(preselection)*. • Only 11.8% of sites met the basic requirements the authors set to be compliant with EU data protection law as a minimum hurdle.
	Matte, Bielova and Santos (2020[78]).	Semi-automatic crawl of consent notices on 560 websites of French, Italian or English-speaking countries	• 46.5% websites nudged consumers towards accepting consent by pre-selecting options *(preselection)*. • 12.3% of websites registered positive consent even if the consumer had not made a choice *(preselection)*. • 7.7% websites stored a positive consent even if the consumer explicitly opted out. • Overall, there was at least one violation of the GDPR or EU Privacy Directive in 54% of the sample of websites.
	Soe et al (2020[80])	Manual analysis of 300 consent notices in a selection of Scandinavian and English language news outlets	• Almost all websites (297 or 99%) used dark patterns when eliciting consent from consumers. • Most dark patterns were either of the obstruction type (43%) or interface interference (45.3%) type. The remainder were classified as forced action or nagging, and no sneaking dark patterns were identified.
	Utz et al. (2019[77])	Manual inspection of the user interface of a random sample of 1 000 notices relating to the 500 most popular websites of each EU member state ranked by Alexa	• 57.4 % of consent notices in the sample used interface design to steer website visitors towards accepting privacy-unfriendly settings. • Typical techniques identified included highlighting in colour the button to accept privacy-unfriendly defaults *(false hierarchy)*, hiding advanced settings behind hard-to-see links *(hidden information or hard to cancel/opt out)*, and pre-selecting checkboxes that activate data collection *(preselection)*. • 95.8% of consent notices provided either no consent choice or confirmation only (*hard to cancel/opt out*).
Major online platforms	Forbrukerrådet (2021[86])	Mystery shopping focusing on Amazon and its Prime service	• Amazon was found to allow consumers to sign up to its Prime service very easily but employ misdirection and visual interference to create obstacles to cancelling the service. A consumer needed to go through many more screens to cancel the service and was constantly encouraged to stop the cancellation process and retain the Prime service, including through emotive language *(hard to cancel/opt out, confirmshaming/toying with emotion)*.

	CMA (2020[85]).	Identification of certain dark patterns on online platforms covered by inquiry	Examples of dark patterns identified fell into three broad categories: • Lack of accessibility and clarity. For example, the CMA found Google and Facebook presented consumers with a large number of options in relation to their privacy settings in multiple locations *(hidden information)*. • Lack of balance, including: o use of visually prominent options, such as a "Next" blue button in Google's Android sign up process encouraging the consumer to click it rather than consider privacy policy and terms *(false hierarchy)*. o use of positive or negative language, including by Google, Microsoft and Facebook, to promote benefits or disbenefits or certain choices to the consumer, e.g. Google warning consumers from turning off Ad Personalisation in Google Search that they will "still see ads, but they'll be less useful" *(confirmshaming/toying with emotion)*. o use of defaults for ad personalisation, including by Facebook, Bing, Snapchat and Twitter *(preselection)*. • Lack of consistency and not enabling consumer choices. For example, the CMA found platforms, including Google, Facebook, Instagram, and Bing, made it hard for consumers to engage with privacy settings in a consistent manner *(hard to cancel/opt out)*.
	ACCC (2019[84]).	Identification of certain dark patterns on online platforms covered by inquiry (Gmail, Facebook, Twitter and Apple Store)	• When "Ad personalisation" was turned on in Google's ad settings, there was a pre-selected checkbox for "Also use your activity and information from Google services to personalise ads on websites and apps that partner with Google to show ads. This stores data from websites and apps that partner with Google in your Google Account" *(preselection)*. • None of the digital platforms reviewed required consumers to review and edit their default data and privacy controls before the creation of a new account, such that they would automatically be configured to default settings *(preselection)*. • Confirming the Norwegian Consumer Council's findings, several elements of Google's user interface design were found to discourage or prevent consumers from opting out of Google's collection of their location data *(hard to cancel/opt out)*.
	Forbrukerrådet (2018[27]).	Mystery shopping to analyse a sample of privacy-related settings in Facebook, Google and Windows 10	All three companies were found to make use of practices involving privacy-intrusive default settings, misleading wording, giving consumers an illusion of control, hiding away privacy-friendly choices, take-it-or-leave-it choices, and choice architectures where choosing the privacy friendly option required more effort from the consumer. Key findings included that: • Facebook and Google had privacy-intrusive defaults *(preselection)*, and consumers who desired a privacy-friendly option would need to go through a significantly longer process *(hard to cancel/opt out)*. • Popups from Facebook, Google and Windows 10 had design and wording that nudged users away from privacy-friendly choices *(false hierarchy, confirmshaming)*. • Choices were worded to compel users to make certain choices, while key information was omitted or downplayed *(confirmshaming, hidden information)*. • Facebook and Google threatened loss of functionality or deletion of accounts if consumers did not choose the privacy-intrusive option *(forced disclosure)*.
	Forbrukerrådet (2018[83]).	Mystery shopping focusing on Google and its location tracking practices	Google was found to use various dark patterns to steer consumers into privacy-intrusive settings regarding location history, including: • Enabling location tracking by default, through a hidden default setting ("Web & Activity") *(preselection)*. • Hiding information needed to make an informed choice about location tracking *(hidden information)*. • Employing a deceptive click-flow on a mobile device to make it easier to agree to tracking and hard to disagree *(hard to cancel/opt out)*. • Repeated nudging to enable location tracking *(nagging)*. • Requiring location tracking to be turned on to use other bundled services *(forced disclosure)*.

	Cases of enforcement action against online platforms	-	Examples include (further examples detailed in Annex G): • The US FTC's action against Amazon, Apple and Google in 2016 for hidden in-app charges. • The CNIL's action against Google (2019) for pre-selecting consent to ad personalisation and making it hard to find relevant information. • EU consumer authorities' action against Booking and Expedia (2020) for hidden charges and misleading scarcity claims. • EU consumer authorities' action against Google (2021) for hidden charges and hidden information.
Search engines and browsers	ACCC (2021[87])	Identification of certain dark patterns in search engines and browsers covered by inquiry	The ACCC identified examples of dark patterns during its review of the consumer journeys to change search engines and browsers: • While downloading the Ecosia search engine browser extension on Microsoft Edge, the ACCC found that Edge turned off the extension, thus disabling choices made by consumers *(hard to cancel)*. This occurred after a consumer twice confirmed their decision to add the extension to their browser, and confirmed that the extension could access and change certain settings *(nagging)*. • To change the pre-set search engine on Edge on a desktop device, users had to navigate multiple screens to access the required setting *(preselection, hard to cancel/opt out)* • During the process of downloading the Ecosia extension to Chrome, Google presented a pop-up message to users stating that the browser extension can "read and change your data..." and "read a list of your most frequently visited websites" *(toying with emotions)*. Google also gave two options to users: "Add extension" or "Cancel', with the "Cancel" option displayed more prominently *(false hierarchy)*.

Source: Summary based on sources in table. In some cases, for the purposes of clarity, the type of dark pattern identified in the research in question is explicitly noted in parenthesis. (*) denotes that percentages were calculated for the purposes of this table based on numbers presented in the relevant research.

Annex D. Selected evidence of effects of dark patterns on consumer decision-making and of dark patterns' detectability

Source	Methodology	Key findings
EC (2022[29])	Online survey-based experiment involving 7 430 participants in Bulgaria, Germany, Italy, Poland, Spain and Sweden testing the impact of three dark patterns – i) hidden information, ii) toying with emotions and iii) toying emotions combined with personalisation – on their decision-making. The experiment tested whether exposure to dark patterns led participants to make a choice they would not otherwise, which would thus be inconsistent with their preferences. Furthermore, half of the participants were placed in a state of situational vulnerability through time pressure, while the other half was placed in a state of motivated delay, which was a proxy for an "average", "reasonably circumspect and well-informed" consumer.	• All three dark patterns tested led to some consumers making decisions inconsistent with their preferences, with "hidden information" increasing the degree of inconsistency the most of the three. • Participants in a situational vulnerability due to time pressure were more likely to make inconsistent choices (50.89%) than "average" consumers (47.24%) when exposed to dark patterns. • For the three dark patterns "hidden information", "toying with emotions" and "toying with emotions combined with personalisation", preference inconsistency was respectively 12.25, 6.02 and 9.84 percentage points higher for the "average" consumer, and respectively 5.80, 4.16 and 5.50 percentage points higher for the vulnerable consumer. • Results also showed some sub-groups of the population were more likely to make inconsistent choices, specifically older participants and those with lower education levels.
SERNAC (2022[106])	Online field experiment testing different options for informing of and requesting consumers' consent for the use of additional cookies during their browsing, conducted on SERNAC's website with 70 208 unique users. Five "prototypes" representing different personal data protection standards were designed and tested against a control set-up. These included alterations in the way consent was sought for the use of additional cookies, such as i) information about the use and purpose of cookies, ii) modifying default options (opt-in/opt-out) and iii) aesthetic framing, i.e. highlighting options that motivate or discourage decisions about accepting additional cookies.	• Aesthetic framing involving highlighting options inducing consumers to reject additional cookies increased the probability of consumers rejecting cookies by 94 percentage points. • Requiring consumer consent by default, such that consumers must actively choose to accept them (opt-in), increased the probability of consumers rejecting cookies by 86 percentage points. • Use of information notices incorporating links to the website's cookie policy was ineffective, with only 1.4% of users accessing the link allowing cookies to be edited.
Sin et al (2022[96])	Online survey-based experiment with 1 342 participants testing the effects of three dark patterns – two relating to scarcity (high-demand and limited quantity messages) and one relating to social proof (testimonials) – on purchase impulsivity, within a hypothetical single product online shopping context.	• For all three dark patterns tested, average purchase impulsivity for the treatment group was higher than for the control group, with statistical significance, albeit the effect size was small. • Additionally, there was no statistically significant difference detected between the effect size of each dark pattern, meaning they were equally effective.

DITP & DGCCRF (2021[110])	Online field experiment involving use of a fake Facebook advertisement and dark patterns (false activity notifications, false scarcity and urgency claims and false testimonials/guarantees) to steer consumers into buying a fake coffee machine, followed up by survey questions. Participants who attempted to buy the coffee machine were then randomly sorted into three groups: i) a control group, who were told only at the end of the experiment that the ad was fake; ii) an "awareness" group, who were told immediately they had been exposed to a fake ad, encouraged to be more careful and redirected to consumer tips on the DGCCRF's website; and iii) and "awareness and integrated training" group, who, in addition to the treatment applied to group ii), were given special training. In a follow-up phase, participants of all three groups were exposed to advertising for a second fake product by Facebook and email to test the effectiveness of the awareness and training measures.	• 2 542 participants attempted to buy the coffee machine on the website of the coffee machine seller after clicking the Facebook advertisement, corresponding to 12.7% of the website's total visitors. • 1.1% and 0.8% of participants in the "awareness" and "awareness and integrated training" groups respectively fell prey to the second fake product, compared to 1.5% in the control group, corresponding to a reduction of 27% and 47% respectively in the propensity to be tricked. However, results were not statistically significant at the 95% confidence level and hence are to be considered indicative. • More than 9 out of 10 participants in the follow-up survey considered the experimental approach employed to be appropriate for an awareness campaign concerning online fraud.
Luguri and Strahilevitz (2021[25])	Online survey-based experiment with 1 963 participants followed up by survey questions regarding participants' moods. Participants were sorted into either a control group, or a treatment group exposed to "mild" dark patterns (combinations of the hard to cancel / roach motel, false hierarchy, confirmshaming dark patterns) or a treatment group exposed to "aggressive" dark patterns (in addition to the mild dark patterns, further hard to cancel / roach motel, toying with emotions, nagging, and trick question dark patterns), in conjunction with a hypothetical offer to sign up to a dubious identity and data protection program.	• For participants exposed to mild dark patterns, the acceptance of the program more than doubled to 25.8% over the control group (11.3 %). • When exposed to aggressive dark patterns, the acceptance rate jumped to 41.9 %, i.e. almost quadrupling the acceptance rate. • In both the mild and aggressive conditions, the initial screen offering a choice between "Accept and continue (recommended)" selected by default and "Other options" accounted for most of the acceptances, illustrating the effectiveness of seemingly mild dark patterns. • Subsequent dark patterns then continued to increase the acceptance rate, illustrating the cumulative power of dark patterns.
	Second online experiment with participants exposed to different dark patterns both in the framing of the data protection program (the "content") and how participants were able to accept or decline it (the "form"). Four different dark patterns relating to "content" conditions were applied – hidden information, social proof, scarcity and confirmshaming, and three dark patterns relating to the form were applied – default, recommendation, obstruction. Half of the participants were then assigned a trick question with a double negative asking them to confirm their decision.	• Of the content-related dark patterns, hidden information had the greatest effect, with a doubling of the acceptance rate over the control group (30.1% over 14.8%). Social proof (22.1%) and confirmshaming (19.6%) also raised acceptance rates, while scarcity had no statistically significant impact. • Of the form-related dark patterns, making accepting the default choice (pre-selection) and making it hard to decline (obstruction) both significantly increased acceptance rates (20.1% and 23.6% respectively). However, marking the choice to accept as "recommended" did not have a statistically significant impact. • Combinations of specific dark patterns boosted acceptance rates further, illustrating the power of layering dark patterns. For example, combining hidden information and obstruction dark patterns led to a 34.4% acceptance rate compared to a 13.2% rate for a control group. • The trick question dark pattern had a substantial effect on whether participants accepted or declined the program. For the half that saw the trick question, 19.2% had accepted the program. But after being exposed to the trick question that asked them to "confirm" their answer, 33.4% accepted it.

Graßl et al (2021[94])	Online experimental survey with 228 participants investigating the effects of three dark patterns – "default" (pre-selection), "aesthetic manipulation" (false hierarchy), and "obstruction" (hard to cancel/opt out) - on consumers' consent decisions in cookie consent requests and their perception of control over their personal data.	• Most participants agreed to all consent requests regardless of the dark patterns, meaning that there was no substantial effect of the dark patterns on the outcome consent decision relative to a no-dark patterns scenario. One reason may be that consumers have been conditioned from reviewing consent requests on a daily basis to follow a heuristic of choosing the usual option irrespective of any dark patterns at play. • Dark patterns did not make participants perceive less control over their personal data – instead, obstructing the privacy-friendly option "Do not Agree" with "Manage options" actually led to more rather than less perceived control.
	Online experimental survey with 255 participants, where the direction of the design nudges was reversed in the form of "bright patterns". Specifically, default, aesthetic manipulation and obstruction were designed to favour the privacy-friendly option.	• Obstruction and default bright patterns swayed participants effectively towards the privacy-friendly option: compared to the first experiment, about ten times more participants changed their consent behaviour between conditions in the second experiment.
Strahilevitz (2021[95])	Behavioural experiment to test effectiveness of dark patterns on larger screens versus smaller screens.	• Techniques such as hidden information were found to be much more effective on smaller screens such as smartphones as opposed to bigger screens such as desktop monitors.
Bongard-Blanchy et al. (2021[33])	Survey of 406 participants regarding awareness of single or combinations of dark patterns as follows: a) sneak-basket/false hierarchy, b) autoplay, c) trick question/preselection, d) loss-gain framing/confirmshaming, e) preselection/loss-gain framing, f) hidden information/trick question, g) bundled/forced consent, h) high-demand/limited-time message, and i) confirmshaming.	• Participants were generally cognizant that dark patterns can exert a detrimental influence on them and many were able to recognise them. • Participants under 40 and those with higher education than high school diplomas were more likely to recognise them. • Rates of identification by participants of the dark patterns were as follows: high-demand/limited-time message (84%), confirmshaming (71%), hidden information/false hierarchy (54%), loss-gain framing/confirmshaming (53%), autoplay (49%), trick question/pre-selection (40%), preselection/ loss-gain framing (38%), hidden information/trick question (16%), bundled/forced consent (14%). • Participants who recognised manipulative designs more easily considered themselves slightly less likely to be influenced by them. • However, most individuals could not precisely determine the consequences of dark pattern influence, thus displayed little concern. • Participants' likelihood of being influenced did not correlate with their general awareness.
EC (2020[99])	Online experimental survey in 10 EU countries with 700 participants per country to test the effectiveness, on travel booking websites and apps, of seven commercial practices in influencing the likelihood of selecting a target package, flight or hotel, from five categories: social proof ("Review"- Displaying a high review score of 9.2 and "Recommended" – indicating that an offer was recommended); discount claim ("Reference pricing"- indicating an offer was on sale relative to a reference price and "Best Price Guarantees" - guaranteeing the offer had the best price); pressure selling ("Limited time offer", such as ''Only two seats remaining", and a limited offer); and hidden charges (drip pricing).	• "Review" increased the likelihood of selecting the target option by 25% in the case of package and 29% in the case of hotel. This commercial practice did not apply for flights. • "Recommended" increased the likelihood of selecting the target option by 24%, 18% and 21% in the case of flight, package and hotel respectively. • Reference pricing increased the likelihood of selecting the target option by 4% in the case of flight and package, and 7% in the case of hotel. • "Best price guarantees" increased the likelihood of selecting the target option by 20% in the case of flight, 18% for the package, and 16% in the case of hotel. • Scarcity cues did not have any statistically significant effect in any of the tasks. • Pressure selling decreased the likelihood of selecting the target option by 3% for the hotels, and had no statistically significant effects for the other tasks. • Drip pricing increased the likelihood of selecting the target option by 4% in the case of flight, 6% or the package, and 3% in the case of hotel.

Bhoot, Shinde and Mishra (2020[104])	Survey of 300 participants testing users' ability to identify 12 selected dark patterns and the underlying factors driving the identification.	• While 41.4% of participants claimed to have never been tricked by websites, they were unable to identify all the twelve types of dark patterns and became victims to at least one of them. • 15% of participants were vaguely familiar with the term dark pattern. • Rates of identification by participants of the dark patterns were as follows: forced continuity (88.6%), confirmshaming (82.3%), bait & switch (81.3%), misdirection (73%), hidden cost (69.3%), disguised ads (55.3%), price comparison prevention (52.3%), sneak into basket (47.6%), friend spam (46%), privacy suckering / forced disclosure (40.6%), trick questions (32.6%), roach motel / hard to cancel (18.6%) . • Ability to identify a dark pattern was correlated with the frequency with which the participant had encountered it as well as their level of frustration with it. • The appeal of the design of the dark pattern was correlated with the trustworthiness the participant felt toward it.
Nouwens et al. (2020[79])	Online field experiment with 40 participants to investigate how the eight most common consent notice designs affect consumer decisions.	• Removing the "reject all" button from the first page of a consent pop-up increased consent by 22–23 percentage points *(hard to cancel/opt out)*. • Displaying more granular consent choices on the first page decreased consent by 8–20 percentage points.
Di Geronimo et al. (2020[73])	Online experimental survey of 584 participants to test identification of dark patterns. The survey included videos of popular apps' usage containing five different types of dark patterns pertaining to different top categories: nagging, intermediate currency, false hierarchy, forced action, and sneak into basket. Two videos displaying usage of two apps each containing one dark pattern were randomly assigned to participants, as well as a video of an app containing no dark pattern as a control.	• The majority of participants did not spot malicious designs in the apps containing dark patterns (55%), some were unsure (20%), and the remaining ones found a malicious design in the app (25%). As for the control, 86% of participants recognised that the app had no dark patterns. • The rate of identification of dark patterns was as follows: nagging (30%), false hierarchy (27%), forced action (27%), intermediate currency (25%) and preselection/sneak into basket (14%). • The ability to spot a malicious design was found to be correlated with previous knowledge about dark patterns, but not with age, employment status, or level of education. • After the researchers pointed the dark patterns out to participants, of those who indicated having identified a malicious design only 24% of participants considered their answer correct, while 56% were unsure or considered their malicious design different from the dark pattern shown. Thus these findings tend to confirm a high level of blindness to dark patterns among consumers.
Maier and Harr (2020[103])	Focus groups with 9 participants and interviews with 5 participants, focusing on users' perceptions and experiences of dark patterns presented to the participants.	• Participants were moderately aware of the dark patterns, several of which were perceived as sneaky and dishonest.
Teubner and Graul (2020[97])	Online experimental survey of 265 participants to test perceptions of scarcity and popularity cues on a fictive online accommodation site.	• Both scarcity and popularity cues triggered scarcity perceptions and, in turn, booking intentions, though scarcity cues were found to be the more effective type.
Utz et al (2019[77])	Online field experiment with 36 530 participants, with both mobile and desktop users, to test the effects on consumer cookie consent decisions of the number of choices available to consumers and of nudging via preselection.	• Pre-selection versions of consent notices led to around 30% of mobile users and 10% of desktop users to accept tracking from all third parties. • A highlighted "Accept" button *(false hierarchy)* led to 50.8% mobile and 26.9 % desktop users accepting versus 39.2% mobile and 21.1% desktop in absence of a highlighted "Accept" button. • These results also highlight the greater effectiveness of dark patterns on mobile as opposed to desktop interfaces.
Machuletz and Böhme (2019[93])	Online experimental survey with 150 participants testing the effects of the number of options and a highlighted default button on consent notices, followed by an exit survey testing perceptions.	• A highlighted default button ("select all") *(false hierarchy)* led participants to accept cookies for more purposes than a control group. • Participants who saw the highlighted default button were also less able to correctly recall their choice. After being reminded of their choice, they regretted it more often and found the consent notice more deceptive than the control group.

Drossos, Zacharioudakis and Dionysiou (2019[98])	Online field experiment with data collected from more than one thousand users who visited more than six hundred different product pages, testing the effect of social proof and scarcity dark patterns on consumer decision-making.	• Both social proof- and scarcity-related dark patterns affected users' behaviours and boosted micro-conversion rates.
Keizer (2017[101])	Online experimental survey of 268 highly educated senior-age regular visitors of opera performances to test the effect of scarcity and social proof on consumer responses within an online opera ticketing store.	• Scarcity was found to have a positive effect on the level of time pressure perceived by participants, but a negative effect on the level of their purchase intentions. • No significant effects of social proof on perceptions of time pressure, perceptions of product value or purchase intentions were found.
Jeong and Kwon (2012[100])	Two in-person experiments with 208 participants to test the effectiveness of a scarcity dark pattern (limited product availability) and social proof dark pattern (popularity claim).	• The popularity claim appeared to enhance quality perception, particularly among highly risk-averse consumers, and purchase intention. These findings were attributed to the quality signalling effect and the bandwagon effect of the claim. • The limited availability claim exerted no influence. Low message credibility and the lack of psychological reactance were deemed to be possible reasons for the insignificant effect of the claim.

Source: Summary based on sources in table. In some cases, for the purposes of clarity, the type of dark pattern identified in the research in question is explicitly noted in parenthesis.

Annex E. Selected evidence of financial loss, psychological detriment and impacts on consumer trust resulting from dark patterns

Name of dark pattern	Source	Key findings regarding evidence of financial loss
Financial detriment		
Friend spam / address book leeching	Class action law suit	LinkedIn was subject to a class action law suit in the US for use of the friend spam dark pattern, involving automatically sending emails to consumers' contacts while making it appear that they came from the consumers themselves.[77] LinkedIn was required to pay out a USD 13 million settlement to affected consumers for the practice. Each affected consumer could receive compensation of up to USD 1 500.
Hidden costs / Drip pricing	Blake et al (2021[109])	A large-scale field experiment on StubHub.com involving several million participants showed that use of drip pricing techniques resulted in consumers spending 21% more than otherwise and being 14% more likely to complete a purchase compared with those who saw all-inclusive prices from the start.
	Rasch, Thöne and Wenzel (2020[122])	According to an experiment, when businesses used drip pricing, consumers were worse off but firms benefited; in contrast, a regulation banning drip pricing led to higher consumer surplus and lower business profits.
	Santana, Dallas and Morwitz (2020[223])	Across six studies, when optional surcharges were dripped (versus revealed up front) consumers were more likely to initially select a lower base priced option which, after surcharges were included, was often more expensive than the alternative.
	Tran (2020[224])	According to a model using web scraped data of posted price transactions on eBay Germany, consumers behaved as if they ignored 12 to 85 percent of the shipping fee, on average, depending on the product analysed. In total, average consumer surplus losses were found to be around 6 per cent.
	US FTC (2017[225])	Separating mandatory resort fees from posted room rates without disclosing the total price was found to be likely to harm consumers by increasing the search costs and cognitive costs of finding and choosing hotel accommodations.
	Robbert and Roth (2014[130])	In a laboratory experiment, drip pricing led consumers to underestimate the total price and to feel deceived by sellers and perceive them as unfair.
	London Economics (2013[226])	Of different price presentation methods assessed in a behavioural experiment, drip pricing led to the highest consumer welfare loss.
	Enforcement action cases	The US FTC took action against Google (in 2014), Apple (in 2014), and Amazon (in 2016) alleging their billing user interfaces for child-directed free apps was unfair because such designs resulted in children racking up charges without parents' knowledge or authorisation. Settlements reached with the three companies required them to fully refund consumers for such charges, resulting in refunds totalling over USD 50 million. [78]
Hidden subscription / forced continuity or hard to cancel	DCCA (2018[227]).	Subscription traps in Denmark were found to result in monthly costs to consumers of up to DKK 699.
	ECC Sweden (2017[69]).	On average, consumers in the six countries reviewed in the study - Belgium, Austria, Sweden, Finland, Norway and the Netherlands - had paid EUR 116 over the last three years as a result of having fallen into an online subscription trap of the type covered in the study.
	Citizens Advice (2016[70])	More than half of respondents to a survey of over 2 000 UK consumers had suffered financial detriment over the year under study from subscription traps, totalling on average between GBP 50 to 100 per person.

	Enforcement action cases	The US FTC in 2020 took action against Age of Learning, Inc., which operates ABCmouse, a digital education program, for misrepresentations about cancellations and failure to disclose important information to consumers, leading tens of thousands of people to be renewed and charged for memberships without proper consent. FTC enforcement actions led to USD 9.7 million in refunds to consumers affected by the practice in 2021.[79]
		The US FTC took action against Commerce Planet, Inc. in 2009 for deceptively pitching consumers a "free" kit with information about how to start a business selling products using online auction sites. Many consumers who ordered the kit were unwittingly enrolled in the program and charged monthly fees without their consent. In 2019 the FTC mailed 53,595 refund checks totalling USD 748 070 to affected consumers.[80]
Several dark patterns	CPRC (2022[111])	In a survey of 2 000 Australian participants, when faced with dark patterns 20% reported having spent more than intended, 17% reported having been pressured into buying something and 9% reported accidentally buying something.
	DITP & DGCCRF (2021[110])	In an online field experiment, 2 542 French consumers attempted to buy a fake coffee machine as a result of Facebook advertisements featuring dark patterns, which would have resulted in total losses for those consumers of EUR 150 000 over the course of less than four weeks.
	Huck and Wallace (2015[229])	Of six different price frames tested in a laboratory experiment – reference pricing, drip pricing, time-limited offers, complex (non-linear pricing), and baiting – both drip pricing and time-limited offers led to the most average consumer welfare loss, of 22% relative to a baseline price frame.
	Ahmetoglu, Furnham and Fagan (2014[102])	In a review of six pricing strategies – drip pricing, reference pricing, the use of the word "free", bait pricing, bundling and time-limited offers – the former three were found to have a robust impact on consumer perceptions and behaviour, particularly in terms of increased purchase intentions and lower search intentions.
	Enforcement action case	The UK CMA investigated hotel booking sites in 2017 for misleading activity messages and scarcity claims, misleading discount claims, incorrect referencing pricing and hidden charges. It subsequently received formal commitments from the sites to bring their practices in line with UK consumer laws, with resulting benefits to consumers estimated at GBP 34 million (OECD, 2021[9])
Psychological detriment and impacts on trust		
Several dark patterns	EC (2022[29])	A lab experiment conducted in Italy, Germany and Spain tested 120 participants' neurophysiological and psychological reactions to three combinations of dark patterns while trying to complete a task: i) forced action combined with an element of personalisation; ii) confirmshaming; and iii) interface interference involving preselection and a trick question. "Forced action combined with personalisation" not only hampered the extent to which participants could successfully complete a common day-to-day task online, but also increased their heart rate, possibly linked to increased anxiety and alertness. It also led to the highest levels of manipulation and frustration reported by the participants. With "confirmshaming", participants had no issues completing the task nor significant emotional effects, suggesting a degree of habituation towards the practice. While the ability of participants to complete the task was negatively affected from "interface interference", no significant neurophysiological effects were detected. However, the time spent on the task increased and their information comprehension levels were significantly lowered.
	CPRC (2022[111])	In a survey of 2000 Australian participants, 83% of participants experienced one or more negative consequences as a result of a website or app using design features aimed at influencing their behaviour, 40% felt annoyed and 28% felt manipulated when using a website or app with a dark pattern.
	Luguri and Strahilevitz (2021[25])	When asked about their mood following a behavioural experiment, participants exposed to mild dark patterns or none at all felt similar levels of negative affect, while those exposed to aggressive dark patterns were significantly more upset and were much more likely to drop out of the study. Overexposure to dark patterns may therefore irritate consumers and cause them to disengage, whereas mild dark patterns may not elicit much affective response while still substantially increasing uptake.
	Voigt, Schlögl and Groth (2021[118])	In an online survey-based experiment of 204 participants, a higher level of perceived annoyance was identified with participants who used the dark pattern version of an online shop. A significant connection between perceived annoyance and participants' expressed brand trust was also identified.
	Gray et al. (2021[119])	In a survey of 169 participants, when asked about their felt emotions in relation to past manipulative digital product experiences, participants frequently expressed they felt strong emotions such as being distressed, upset, hostile and irritable.
	Maier and Harr (2020[103])	In qualitative research focusing on participants' perceptions and experiences with dark patterns, participants expressed a resigned attitude toward such techniques and primarily blamed businesses for their occurrence.

Scarcity and/or social proof claims	Shaw (2019[120])	In a survey of 2102 British participants regarding scarcity and social proof claims on hotel booking websites, 65% of participants interpreted examples of scarcity and social proof claims used by hotel booking websites as sales pressure; 49% said they were likely to distrust the company as a result of seeing them; 16% said they believed the claims; and 34% expressed a negative emotional reaction to these messages, such as contempt and disgust.
	Kristofferson et al. (2017[121])	In seven different studies examining the effects of limited-quantity scarcity promotions on consumer aggression in different contexts, exposure to limited-quantity scarcity promotions was found to lead consumers to behave more aggressively.

Source: Summary based on sources in table

Annex F. EU legislation that may address selected dark patterns

Name of dark pattern	Relevant legislation
Nagging	UCPD Annex 1 Practice 26 (Making persistent and unwanted solicitations by telephone, fax, e-mail or other remote media) UCPD Art. 8-9 Aggressive practice (harassment), including Art. 9(b) (use of threatening or abusive language or behaviour) DMA (anti-circumvention rule)
Activity messages	UCPD Art. 6 Misleading action (availability, quantity) UCPD Annex 1 Practices 7 (Falsely stating that a product will only be available for a very limited time, or that it will only be available on particular terms for a very limited time, in order to elicit an immediate decision and deprive consumers of sufficient opportunity or time to make an informed choice) and 18 (Passing on materially inaccurate information on market conditions or on the possibility of finding the product with the intention of inducing the consumer to acquire the product at conditions less favourable than normal market conditions)
Testimonials	UCPD Annex 1 Practices 23b (Stating that reviews of a product are submitted by consumers who have actually used or purchased the product without taking reasonable and proportionate steps to check that they originate from such consumers) and 23c (Submitting or commissioning another legal or natural person to submit false consumer reviews or endorsements, or misrepresenting consumer reviews or social endorsements, in order to promote products) UCPD Art. 7(6) Misleading omission (Where a trader provides access to consumer reviews of products, information about whether and how the trader ensures that the published reviews originate from consumers who have actually used or purchased the product shall be regarded as material)
Hard to cancel / roach motel	UCPD Art. 8 Aggressive practice (coercion), including Art. 9(d) (impose onerous or disproportionate non-contractual barriers where a consumer wishes to exercise rights under the contract, including rights to terminate a contract or to switch to another product or another trader) UCPD Art. 7 Misleading omission (right of withdrawal) CRD Art. 6(1)(h) (right of withdrawal), Art. 10 and Art. 14(2), (4) (consequences) UCTD Annex point 1(h) (Automatically extending a contract of fixed duration where the consumer does not indicate otherwise, when the deadline fixed for the consumer to express this desire not to extend the contract is unreasonably early) and point 1(i) (Irrevocably binding the consumer to terms with which he had no real opportunity of becoming acquainted before the conclusion of the contract) DMA (anti-circumvention rule)
Price comparison prevention	UCPD Art. 6 Misleading action (overall presentation, comparative advertising) UCPD Art. 7 Misleading omission (price as material information)
Intermediate currency	UCPD Art. 6 Misleading action (price, main characteristics) UCPD Art. 7 Misleading omission (price, main characteristics) UCPD Art. 8-9 Aggressive practice (undue influence, in particular in case of vulnerable consumers such as young people) CRD Art. 6(1)(e) (price, main characteristics)

Sneak into basket	UCPD Annex 1 Practice 29 (Demanding immediate or deferred payment for or the return or safekeeping of products supplied by the trader, but not solicited by the consumer) CRD Art. 27 (inertia selling consequences - consumers exempted from the obligation to provide consideration for unsolicited products; absence of a response from the consumer is not consent)
Hidden costs	UCPD Art. 6 Misleading action (price) UCPD Art. 7 Misleading omission (price, hiding or providing in an untimely manner) CRD Art. 6(1)(e) (price) CRD Art. 22 (trader need the consumers' express consent for any extra payment in addition to the remuneration agreed upon for the trader's main contractual obligation) UCTD Art. 4(2), Art. 5 (plain intelligible language; consumer must be put in a position to clearly understand the economic consequences stemming from the contract (e.g. Case C-609/19))
Hidden subscription / forced continuity	UCPD Art. 7 Misleading omission (hiding, ambiguity on main characteristics, price, right of withdrawal and cancellation) UCPD Art. 6 Misleading action (main characteristics, price) UCPD Art. 8-9 Aggressive practice (coercion) CRD Art. 6 (price, main characteristics, right of withdrawal), Art. 8(2) (information must be provided in a clear and prominent manner before placing the order) UCTD Annex 1h (Automatically extending a contract of fixed duration where the consumer does not indicate otherwise, when the deadline fixed for the consumer to express this desire not to extend the contract is unreasonably early)
Bait and switch	UCPD Art. 6 Misleading action (existence and characteristics of the product) UCPD Art. 7 Misleading omission (hiding, untimely information) UCPD Annex 1 Practice 5 (Making an invitation to purchase products at a specified price without disclosing the existence of any reasonable grounds the trader may have for believing that he will not be able to offer for supply or to procure another trader to supply, those products or equivalent products at that price for a period that is, and in quantities that are, reasonable having regard to the product, the scale of advertising of the product and the price offered) UCPD Annex 1 Practice 6 (Making an invitation to purchase products at a specified price and then: (a) refusing to show the advertised item to consumers; or (b) refusing to take orders for it or deliver it within a reasonable time; or (c) demonstrating a defective sample of it, with the intention of promoting a different product)
Hidden information / False hierarchy	UCPD Art. 6 Misleading action (characteristics, price, consumers' rights, overall presentation of information) UCPD Art. 7 Misleading omissions (hiding, unclear, ambiguous, untimely) CRD Art. 6, Art. 8 (pre-contractual information must be clear and comprehensible) GDPR Art. 5(1) data protection principles, in particular of transparency, fairness, Art. 25 data protection by design and default DMA (anti-circumvention rule)
Preselection (default)	UCPD Art. 6 Misleading action (the need of a service) UCPD Art. 8 Aggressive practice (coercion, undue influence) CRD Art. 22 (express consent of a consumer for additional charges cannot be inferred by using default options) GDPR Art. 5(1) data protection principles, in particular of transparency, fairness, Art. 25 data protection by design and default, depending on circumstances also Art. 4(11) and Art. 7 conditions of consent (pre-ticked boxes do not constitute valid consent under the GDPR - C-673/17) DMA (anti-circumvention rule)
Toying with emotion	UCPD Art. 6 Misleading action (characteristics, benefits and risks of product) UCPD Art. 8-9 Aggressive practice (coercion, undue influence), including Art. 9(b) (Use of threatening or abusive language or behaviour) and Art. 9(c) (Exploitation by the trader of any specific misfortune or circumstance of such gravity as to impair the consumer's judgement, of which the trader is aware, to influence the consumer's decision with regard to the product) UCPD Annex 1 Practices 28 (Including in an advertisement a direct exhortation to children to buy advertised products or persuade their parents or other adults to buy advertised products for them) and 30 (Explicitly informing a consumer that if he does not buy the product or service, the trader's job or livelihood will be in jeopardy)

	GDPR Art. 5(1) data protection principles, in particular of transparency, fairness, Art. 25 data protection by design and default AVMSD Art. 9(1)(b) (bans subliminal techniques), 9(1)(g) (bans manipulation of minors)
Trick questions	UCPD Art. 6 Misleading action (existence and characteristics of product) UCPD Art. 7 Misleading omissions (unintelligible, ambiguous information) UCTD Art. 4(2) and Art. 5 (contract terms must be in plain and intelligible language) GDPR Art. 5(1) data protection principles, including of transparency, fairness, Art. 25 data protection by design and default DMA (anti-circumvention rule)
Disguised ad	UCPD Art. 6 Misleading action (marketing) UCPD Art. 7(2) Misleading omission (failure to disclose commercial intent) UCPD Annex 1 Practices 11 (Using editorial content in the media to promote a product where a trader has paid for the promotion without making that clear in the content or by images or sounds clearly identifiable by the consumer) and 11a (Providing search results in response to a consumer’s online search query without clearly disclosing any paid advertisement or payment specifically for achieving higher ranking of products within the search results) and Practice 28 (Including in an advertisement a direct exhortation to children to buy advertised products or persuade their parents or other adults to buy advertised products for them) UCPD Art. 8-9 Aggressive practice (undue influence) UCPD, AVMSD, eCommerce Directive, DSA (advertisement and commercial communications must be clearly recognised) ePrivacy Directive Art. 13 (unsolicited communications)
Confirmshaming	UCPD Art. 6 Misleading action (need for a service, results to be expected) UCPD Art. 8-9 Aggressive practice (undue influence), including Art. 9(b) (Use of threatening or abusive language or behaviour) and Art. 9(d) (Any onerous or disproportionate non-contractual barriers imposed by the trader where a consumer wishes to exercise rights under the contract, including rights to terminate a contract or to switch to another product or another trader)
Forced registration	UCPD Art. 8 Aggressive practice (coercion) UCPD Annex 1 Practice 24 offline scenario applied to the digital environment (Creating the impression that the consumer cannot leave the premises until a contract is formed) UCTD Annex 1i (Irrevocably binding the consumer to terms with which he had no real opportunity of becoming acquainted before the conclusion of the contract) GDPR Art. 5(1) data protection principles, including of transparency, fairness, Art. 25 data protection by design and default
Low stock / high demand message	UCPD Art. 6 Misleading action (availability, quantity) UCPD Art. 7 Misleading omission (hiding information) UCPD Annex 1 Practices 7 (Falsely stating that a product will only be available for a very limited time, or that it will only be available on particular terms for a very limited time, in order to elicit an immediate decision and deprive consumers of sufficient opportunity or time to make an informed choice) and 18 (Passing on materially inaccurate information on market conditions or on the possibility of finding the product with the intention of inducing the consumer to acquire the product at conditions less favourable than normal market conditions)
Countdown timer / Limited time message	UCPD Art. 6 Misleading action (availability, quantity) UCPD Art. 7 Misleading omission (hiding information) UCPD Annex 1 Practices 7 (Falsely stating that a product will only be available for a very limited time, or that it will only be available on particular terms for a very limited time, in order to elicit an immediate decision and deprive consumers of sufficient opportunity or time to make an informed choice) and 18 (Passing on materially inaccurate information on market conditions or on the possibility of finding the product with the intention of inducing the consumer to acquire the product at conditions less favourable than normal market conditions)
Infinite scroll	Depends on the context of its use and specific circumstances, possibly in breach of UCPD Art 6-7 Misleading practices and Art. 8-9 Aggressive practice (undue influence)
Autoplay	Depends on the context of its use and specific circumstances, possibly in breach of UCPD Art 6-7 Misleading practices and Art. 8-9 Aggressive practice (coercion)

Immortal account	UCPD Art. 7 Misleading omission (hiding, ambiguity on main characteristics, right of withdrawal and cancellation) UCPD Art. 6 Misleading action (main characteristics) UCPD Art. 8-9 Aggressive practice (coercion) CRD Art. 6 (main characteristics, right of withdrawal) GDPR Art. 17 (right to erasure)
Misleading referencing pricing	UCPD Art. 6 Misleading action (existence and characteristics of a product, price, overall presentation) UCPD Art. 7 Misleading omission (hiding, untimely information)
Friend spam	UCPD Art. 6 Misleading action (the motives for the commercial practice, need for a service) GDPR Art. 5(1) data protection principles, including of transparency, depending on circumstances Art. 4(11) and Art. 7 conditions of valid consent for the collection and processing of data ePrivacy Directive Art. 13 (unsolicited communications)
Loot boxes	UCPD Art. 6 Misleading action (main characteristics, price) UCPD Art. 7 Misleading omission (main characteristics, price) UCPD Art. 8-9 Aggressive practice (undue influence, in particular in case of vulnerable consumers such as young people) CRD Art. 6(1) (main characteristics, price, the manner in which the price is to be calculated)

Source: EC (2022[29])

Annex G. Examples of enforcement action and legal complaints against dark patterns in selected OECD jurisdictions

Type of dark pattern	Jurisdiction	Examples of enforcement action or legal complaint
Pre-selection, hidden information, forced disclosure, false hierarchy, hard to cancel/opt out	United States	In 2011, the FTC took action against Facebook for representing to consumers that they could keep their information on Facebook private, then repeatedly allowing it to be shared and made public in various ways. Facebook agreed to the FTC's proposed settlement and to reform its privacy practices.[81]
	European Union (Italy)	In 2018, the Italian Competition Authority (AGCM) fined Facebook EUR 10 million for data practices in breach of the Italian Consumer Code, which implements the UCPD. Inter alia, it considered that Facebook exerted undue influence on registered consumers by pre-selection of the broadest consent to data sharing, and placing restrictions on the use of the website when consumers decided to limit their consent to dissuade them from doing so.[82]
	European Union	Following a report that the Norwegian Consumer Council (NCC) produced on Google's location tracking practices involving hidden information, default settings, deceptive click-flow and nudging regarding location-tracking (as discussed in Annex C) (Forbrukerrådet, 2018[84]), the NCC and seven other European consumer organisations filed legal complaints against Google in 2018 in several jurisdictions for breach of the GDPR, which were transferred to the Irish Data Protection Commission.[83]
	European Union (France)	In 2019, the CNIL fined Google EUR 50 million for data practices in breach of the GDPR. It found Google did not obtain valid consent from consumers, as consent was neither sufficiently informed (because information was diluted across several documents) nor unambiguous (because agreement to ad personalisation was pre-ticked).[84]
	European Union (Germany)	In 2020, the Rostock Regional Court of Germany decided, following a complaint filed by the Federation of German Consumer Organisations (vzbv) against advocado, an online service that helps people find a lawyer, that advocado's use of pre-ticked boxes in cookie banners was in breach of the GDPR, noting cookie banners must give equal prominence to the options of accepting and declining.[85]
	Australia	In 2021, following proceedings brought by the ACCC, the Federal Court of Australia found Google breached the ACL by misleading consumers about personal location data collected, including by failing to inform consumers of certain location-tracking settings ("Web & App Activity") that were turned on by default.[86]
	European Union	In 2021, noyb (European Center for Digital Rights) filed 422 formal GDPR complaints with data protection authorities in 10 EU countries, in relation to dark patterns in cookie consent notices involving, inter alia, a lack of a "reject" button, pre-ticked boxes, and different colours for "accept" and "reject" buttons.[87]
	European Union (France)	In 2022, the CNIL fined Google EUR 150 million and Facebook EUR 60 million for data practices in breach of the GDPR. Specifically, it found the companies did not provide a button allowing the consumer to refuse all cookies as easily as accept them all (i.e. with one click).[88]
	United States	In 2022, Attorneys General from the States of Indiana, Texas and Washington and the District of Columbia sued Google for use of dark patterns to gain access to location-tracking data, even after consumers thought they had disallowed Google from accessing that information.[89]

Misleading reference pricing	Australia	In 2020, following proceedings brought by the ACCC, the Federal Court of Australia found hotel booking site trivago breached the ACL for, inter alia, misleading reference pricing, involving strike-through prices or text in different colours giving consumers a false impression of savings. The Full Federal Court of Australia later dismissed trivago's appeal. [90]
Hidden subscriptions / forced continuity or hard to cancel	Australia	In 2016 the ACCC took action against Fabletics, an exercise clothing retailer, and Scootprice, an online retailer, for covertly signing consumers up to subscriptions after making a single purchase on their websites. Both companies co-operated with the ACCC to make ongoing membership fees clearer.[91]
	United States	In 2016 the FTC took action against BunZai Medi Group, which sold skincare products to consumers, for use of a number of dark patterns. These included pop-up ads that forced consumers to accept an offer, fine print at the end of a transaction that contradicted earlier marketing claims and hidden, difficult to cancel subscriptions masking as "risk-free" trials.[92]
	European Union (Italy)	In 2016, the AGCM fined online dating site Edates EUR 350 000 for breach of the Italian Consumer Code upon finding that, following a free registration to the site or a two-week trial subscription offered at a low price, consumers unknowingly found themselves bound to a six-month premium subscription at a cost of EUR 19 a week.[93]
	United States	In 2017, the FTC took action against AAFE Products Corp., et. al., alleging that the online marketers of cooking gadgets, golf equipment, and other online subscription services deceived consumers into thinking that their offerings were free, without clearly disclosing charges. The companies also misrepresented their return, refund, and cancellation policies, hiding the terms in pages of fine print that consumers could access only through a tiny hyperlink.[94]
	United States	As discussed in Annex E, the FTC successfully took action against Commerce Planet, Inc in 2009 and Age of Learning, Inc. in 2020 for use of subscription traps or making it hard to cancel the service.
	Japan	In 2020, the Consumer Affairs Agency (CAA) took an administrative disposition against GRACE Corporation, a mail-order sales company. GRACE Corporation failed to indicate on its online order entry screen that an order would lead to an application for a subscription contract for dietary supplement products.
	Japan	In 2021, the CAA took an administrative disposition against SUPER BEAUTY LABO, a mail-order distributor of health food products. SUPER BEAUTY LABO failed to clearly indicate on the screen at the final stage of the online order entry process the terms and conditions of the subscription contract and cancellation method, and to allow customers to easily check and correct the contents of their orders.
	European Union, United Kingdom & United States	Following a report by the NCC on dark patterns that it alleged Amazon employed to make it hard for consumers to cancel its Prime service (as discussed in Annex C) (Forbrukerrådet, 2021[87]), in 2021 the NCC filed a legal complaint to the Norwegian Consumer Protection Authority for alleged breaches of the Marketing Control Act, which implements the UCPD. A further 15 consumer organisations in Europe and the US also took action against Amazon based on the report.[95] In 2022, following dialogue with the EC and EU consumer protection authorities, Amazon committed to bringing its cancellation practices in line with EU consumer law by enabling EU and European Economic Area consumers to unsubscribe with just two clicks, using a prominent and clear "cancel button".[96]
Hidden charges / drip pricing	Colombia	In 2014 the Superintendence of Industry and Commerce of Colombia (SIC) fined online travel booking company Despegar COP 12 million for using initial prices in its advertising travel packages that were inconsistent with the final prices when including additional charges.[97]
	United States	As discussed in Annex E, the FTC took action against Google, Apple and Amazon in 2014 for hidden in-app charges directed at children. Google and Apple settled the charges in 2014, and the Amazon matter was resolved in 2016.[98]
	European Union (Netherlands)	In 2015, the ACM took action against World Ticket Center B.V. (WTC) for displaying its airfares and trip prices on its website incorrectly. It found WTC failed to include all mandatory costs in the base price of its airfares, with variable costs not clearly mentioned in the base price, and had optional extras such as travel and cancellation insurances pre-selected. The ACM imposed a fine of EUR 350 000 on WTC and required it to adjust the information on its website to have it comply with the rules.[99]
	Australia	In 2015, following proceedings brought by the ACCC, the Federal Court of Australia found airlines Jetstar and Virgin contravened the ACL by engaging in drip pricing practices. It ordered the airlines to pay a penalty of AUD 200 000 penalty.[100] This followed previous successful action by the ACCC against Airbnb, eDreams, Ticketek and Ticketmaster in relation to failure to appropriately disclose mandatory fees.[101]
	Canada	In 2018, the Competition Bureau Canada took action against Ticketmaster for misleading heading prices that did not incorporate additional fees added later in the transaction process. Ticketmaster was ordered to pay CAD 4.5 million to settle the case.[102]

	Chile	In 2019, SERNAC brought a case against airline JetSmart Airlines for not including boarding fees and taxes in the ticket price.
	United States	In 2019, the FTC took action against FleetCor Technologies, alleging that the company had charged consumers hundreds of millions of dollars in hidden and undisclosed fees, after making false promises that they could save consumers money on their fuel costs.[103]
	European Union	In 2019, following a sweep conducted by EU consumer authorities of e-commerce sites offering a variety of goods, services and digital content, such as clothing or footwear, computer software or entertainment tickets that found 211 websites using drip pricing, consumer authorities took action to ensure such websites complied with EU consumer law.[104]
	European Union	In 2019, following negotiations with the EC and EU consumer authorities, Airbnb improved and clarified the way it presented accommodation offers to consumers to be in line with EU consumer law, including by presenting the total price of an offer in searches inclusive of all applicable mandatory charges and fees.[105]
	European Union	In 2020, following a sweep conducted by EU consumer authorities of e-commerce sites selling clothing and footwear, furniture and household items, and electric appliances, which found instances of drip pricing on a fifth of such websites, EU consumer authorities took action to ensure the websites complied with EU consumer law.[106]
Nagging	European Union	In 2022, EU consumer authorities and the EC sent letters to Whatsapp asking, inter alia, how Whatsapp ensures that consumers can reject the new terms of service, especially as persistent in-app notifications prompt consumers to accept the changes.[107] This followed a complaint filed by BEUC and several of its members against Whatsapp for alleged breaches of EU consumer law owing to persistent, recurrent and intrusive notifications pushing users to accept WhatsApp's policy updates.[108]
Intermediate currency	European Union	In 2021, EU consumer authorities and the EC launched a formal dialogue with TikTok to review its commercial practices and policy.[109] This followed a complaint launched by BEUC for alleged breaches of EU consumer law by Tiktok, including for a virtual currency which users can purchase to buy virtual gifts, for which Tiktok claimed an absolute right to modify the exchange rate between the coins and the gifts.[110]
Urgency combined with other dark patterns (hidden charges, activity messages)	United Kingdom	In 2018, the CMA issued court proceedings to ticket reseller viagogo over concerns it broke UK consumer law due to use of misleading low-stock and activity messages as well as pricing obfuscation, inter alia. This subsequently resulted in a court order obliging the company to change its practices.[111]
	European Union	In 2019, EU consumer authorities identified practices diverging from EU consumer law on travel booking websites Booking.com and Expedia. These included not always including all charges in price quotes, not specifying that indications of number of rooms available only related to offers on the platform, and indicating offers were time-limited even if they remained available after expiry of the offer. Following dialogue between the EC and EU consumer authorities, by December 2020 Booking.com and Expedia had aligned their presentation of offers with EU consumer law.[112]
	Australia	In 2019, following proceedings brought by the ACCC, the Federal Court of Australia found ticket reseller viagogo breached the ACL for claiming tickets were scarce when the scarcity only referred to the tickets available on its platform. It also found viagogo failed to disclose additional fees on its websites. It ordered viagogo to pay a penalty of AUD 7 million.[113]
	Japan	In 2019, the CAA determined that ticker reseller viagogo had caused consumer detriment through false and exaggerated representations, such as countdown clocks. Following the CAA investigation, viagogo undertook a corrective action plan to correct its official Japanese website. The CAA also issued a warning to consumers regarding viagogo's conduct.
	United Kingdom	In 2017, the CMA investigated hotel booking sites Expedia, Booking.com, Agoda, Hotels.com, ebookers and trivago for misleading activity messages and scarcity claims, misleading discount claims, incorrect referencing pricing and hidden charges, inter alia. The six hotel booking sites subsequently gave formal commitments to bring their practices in line with UK consumer laws. By September 2019, the CMA had produced principles to guide businesses offering online accommodation booking services, and another 25 more hotel booking sites had signed up to the principles.[114]
	European Union (Hungary)	In 2020, the Hungarian Competition Authority imposed a fine of HUF 2.5 billion on Booking.com for, among other things, misleadingly advertising some of its accommodations with a free cancellation option and exerting undue psychological pressure on consumers to make early bookings, including activity notifications.[115]
	United States	In 2014, the FTC and the Illinois and Ohio State Attorneys General took action against One Technologies, LP, alleging that the company lured consumers with "free" access to their credit scores and then billed them a recurring charge for a credit monitoring service they never ordered.[116]

Bait and switch	United States	In a 2019 settlement with the FTC, Facebook agreed to cease its practice of using consumers' phone numbers originally sought for two-factor authentication for targeted advertising purposes.[117]
Disguised ads and false testimonials	United States	In 2016 the FTC took action against LeadClick Media, an internet advertising company that used ads disguised as news and false testimonials to promote an internet retailer's weight-loss and colon-cleanse products. LeadClick Media was held liable for the deceptive marketing.[118]
Activity messages	United States	In 2014, the FTC took action against online dating company JDI Dating Ltd., alleging that the company used fake profiles to lure consumers into paid memberships and then charged consumers automatic renewal fees without consent.[119]
	United States	In 2019 the FTC took action against Match Group, owner of Match.com, for using love interest advertisements from fake accounts to trick consumers into buying subscriptions to Match.com[120]
Combination of dark patterns	United States	In 2012 the FTC took action against AMG Capital Management, a provider of payday loans via a subscription service, which used multiple dark patterns to deceptively lure consumers into taking on more loans. These included forced continuity (a costly renewal of the loan by default subscription), hard to cancel (avoiding the expensive renewal was more difficult than accepting it), hidden costs (hiding the costs of the renewal behind dense text), preselection (making renewal of the loan the default option), and trick questions (making descriptions of options for the consumer hard to understand). As a result of the action, Scott Tucker, who ran the company, was subsequently barred from engaging in any further lending.[121]

Source: Sources indicated in endnotes. Selected cases in the US also draw on Luguri and Strahilevitz (2021[25]).

References

ACCC (2022), *Digital platform services inquiry. Discussion paper for interim report No.5: Updating competition and consumer law for digital platform services*. [151]

ACCC (2021), *Digital platform services inquiry. Interim report No. 2 - App marketplaces*. [91]

ACCC (2021), *Digital platform services inquiry. Interim report No. 3 - Search defaults and choice screens*. [87]

ACCC (2019), *Digital platforms inquiry. Final report*. [84]

ACM (2021), *Effective online information. Studies on the improvement of online information for consumers*. [181]

ACM (2020), *Guidelines on the protection of the online consumer*. [20]

ACM (2020), *Position Paper. Oversight of algorithms*. [44]

Acquisti, A. et al. (2017), "Nudges for Privacy and Security", *ACM Computing Surveys (CSUR)*, Vol. 50/3, https://doi.org/10.1145/3054926. [68]

AFM & ASIC (2019), *Disclosure: Why it shouldn't be the default*. [177]

Ahmetoglu, G., A. Furnham and P. Fagan (2014), "Pricing practices: A critical review of their effects on consumer perceptions and behaviour", *Journal of Retailing and Consumer Services*, Vol. 21/5, pp. 696-707, https://doi.org/10.1016/j.jretconser.2014.04.013. [102]

Akerlof, G. and R. Shiller (2016), *Phishing for Phools*, Princeton University Press, https://doi.org/10.2307/j.ctvc777w8. [128]

Alavi, T. (2020), *Gray Patterns in UX: where do we draw the line between helpful vs. harmful design?*, https://uxdesign.cc/gray-patterns-in-ux-where-do-we-draw-the-line-between-helpful-vs-harmful-design-ced7fbaa8ad5. [59]

Amazeen, M. (2021), "Native Advertising in a Mobile Era: Effects of Ability and Motivation on Recognition in Digital News Contexts", *Digital Journalism*, https://doi.org/10.1080/21670811.2020.1860783. [41]

Bar-Gill, O., D. Schkade and C. Sunstein (2019), "Drawing false inferences from mandated disclosures", *Behavioural Public Policy*, Vol. 3/02, pp. 209-227, https://doi.org/10.1017/bpp.2017.12. [178]

Beattie, A., C. Lacey and C. Caudwell (2020), *"It's Like the Wild West": User Experience (UX) Designers on Ethics and Privacy in Aotearoa New Zealand*. [46]

Bell, B. and D. Fitton (2021), *Dark Patterns in Mobile Games: A Source of Online Risk for Youths?*. [137]

Berbece, S. (2019), "'Let There Be Light!' Dark Patterns Under the Lens of the EU Legal Framework", *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.3472316. [142]

BEUC (2022), *"DARK PATTERNS" AND THE EU CONSUMER LAW ACQUIS. Recommendations for better enforcement and reform*. [141]

Bhoot, A., M. Shinde and W. Mishra (2020), "Towards the identification of dark patterns: An analysis based on end-user reactions", *IndiaHCI '20: Proceedings of the 11th Indian Conference on Human-Computer Interaction*, pp. 24-33, https://doi.org/10.1145/3429290.3429293. [104]

Bizer, G. and R. Schindler (2005), "Direct evidence of ending-digit drop-off in price information processing", *Psychology and Marketing*, Vol. 22/10, pp. 771-783, https://doi.org/10.1002/MAR.20084. [62]

Blake, T. et al. (2021), "Price Salience and Product Choice", *Marketing Science*, Vol. 40/4, p. 43, https://doi.org/ttps://doi.org/10.1287/mksc.2020.1261. [109]

BMUV (2021), *Code of Corporate Digital Responsibility*. [203]

Bongard-Blanchy, K. et al. (2021), "I am Definitely Manipulated, even When I am Aware of it. It's Ridiculous! - Dark Patterns from the End-User Perspective", *Designing Interactive Systems Conference 2021*, pp. 763-776, https://doi.org/10.1145/3461778.3462086. [33]

Bösch, C. et al. (2016), "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns", *Proceedings on Privacy Enhancing Technologies*, Vol. 2016/4, pp. 237-254, https://doi.org/10.1515/popets-2016-0038. [21]

Botta, M. and K. Wiedemann (2019), "The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey", *Antitrust Bulletin*, Vol. 64/3, pp. 428-446, https://doi.org/10.1177/0003603X19863590. [188]

Brett, L. (2021), *Comments at US FTC workshop "Bringing Dark Patterns to Light"*. [202]

Brignull, H. (2021), *Comments at US FTC workshop "Bringing Dark Patterns to Light"*. [45]

Brignull, H. (n.d.), *Types of Dark Pattern*, https://www.deceptive.design/types. [11]

Brownlee, J. (2016), *Why Dark Patterns Won't Go Away*, https://www.fastcompany.com/3060553/why-dark-patterns-wont-go-away. [52]

Bunker, G. (2013), *The ethical line in user experience research*, https://mumbrella.com.au/the-ethical-line-in-user-experience-research-163114. [207]

Calo, R. (2014), "Digital market manipulation", *George Washington Law Review*, Vol. 82/4, pp. 995-1051, https://doi.org/10.2139/ssrn.2309703. [18]

Cara, C. (2019), "Dark Patterns in the Media: a Systematic Review", *Network Intelligence Studies*, Vol. VII/14, pp. 105-113, https://www.researchgate.net/publication/341105338. [32]

Chivukula, S. et al. (2020), "Dimensions of UX Practice that Shape Ethical Awareness", *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, https://doi.org/10.1145/3313831.3376459. [206]

Chugh, B. and P. Jain (2021), "Unpacking dark patterns: Understanding dark patterns and their implications for consumer protection in the digital economy", *RGNUL Student Research Review*, [134] Vol. 7/1, http://rsrr.in/wp-content/uploads/2021/04/UNPACKING-DARK-PATTERNS-UNDERSTANDING-DARK.pdf.

Citizens Advice (2016), *Locked in. Consumer issues with subscription traps*, https://www.citizensadvice.org.uk/about-us/our-work/policy/policy-research-topics/consumer-policy-research/consumer-policy-research/locked-in-consumer-issues-with-subscription-traps/. [70]

Citron, D. and D. Solove (2022), “Privacy Harms”, *Boston University Law Review*, Vol. 102/793, pp. 793-863, http://dx.doi.org/10.2139/ssrn.3782222. [113]

CMA (2022), *Evidence review of Online Choice Architecture and consumer and competition harm*. [167]

CMA (2022), *Online Choice Architecture. How digital design can harm competition and consumers*. [31]

CMA (2021), *Algorithms: How they can reduce competition and harm consumers*. [19]

CMA (2020), *Online platforms and digital advertising - Market study final report*. [85]

CMA (2020), *Online platforms and digital advertising - Market study. Appendix Y: choice architecture and Fairness by Design*. [235]

CMA (2018), *Tackling the loyalty penalty*. [160]

CMA (2017), *Online hotel booking*, https://www.gov.uk/cma-cases/online-hotel-booking. [192]

CMA & ICO (2021), *Competition and data protection in digital markets: a joint statement between the CMA and the ICO*. [189]

CNIL (2020), *Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l’application de l’article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d’un utilisateur (notamment aux «cookies et autres traceurs») et abrogeant la délibération n°2019-093 du 4 juillet 2019*. [169]

CNIL (2020), *Délibération n° 2020-092 du 17 septembre 2020 portant adoption d’une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux «cookies et autres traceurs»*. [161]

CNIL (2019), “Shaping Choices in the Digital World - From dark patterns to data protection: the influence of ux/ui design on user empowerment”, *IP Reports*, Vol. 6. [112]

CNIL (n.d.), *Données & Design. Co-building user journeys compliant with the GDPR and respectful of privacy*, https://design.cnil.fr. [174]

Cohen, J. (2019), “Bringing Down the Average: The Case for a “Less Sophisticated” Reasonableness Standard in US and EU Consumer Law”, *Loyola Consumer Law Review*, Vol. 32/1, p. 1, https://lawecommons.luc.edu/lclr/vol32/iss1/2. [187]

ConPolicy (2020), *Innovatives Datenschutz-Einwilligungsmanagement - Ablschlussbericht (Innovative Data Protection Consent Management - Final Report)*. [165]

Consumer Reports Digital Lab (2021), *Model State Privacy Act*, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf. [182]

Conti, G. and E. Sobiesk (2010), "Malicious Interface Design: Exploiting the User", *Proceedings of the 19th international conference on World wide web - WWW '10*, https://doi.org/10.1145/1772690.1772719. [22]

Corones, S. et al. (2016), *Comparative analysis of overseas consumer policy frameworks*, Commonwealth of Australia, Australia, https://eprints.qut.edu.au/95636/1/95636.pdf. [184]

Costa, E. and D. Halpern (2019), *The behavioural science of online harm and manipulation, and what to do about it*. [152]

CPRC (2022), *Duped by Design. Manipulative online design: Dark patterns in Australia*. [111]

CPRC (2020), *UNFAIR TRADING PRACTICES IN DIGITAL MARKETS-EVIDENCE AND REGULATORY GAPS*. [148]

Dapde (n.d.), *Obstacles*, https://dapde.de/en/dark-patterns-en/types-and-examples-en/hindernisse2-en/. [26]

Day, G. and A. Stemler (2020), "Are Dark Patterns Anticompetitive?", *Alabama Law Review*, Vol. 72/1, https://doi.org/10.2139/ssrn.3468321. [125]

DCCA (2018), *Misleading consumers online is a cross-border issue*. [228]

de Marcellis-Warin, N. et al. (2022), "Artificial intelligence and consumer manipulations: from consumer's counter algorithms to firm's self-regulation tools", *AI and Ethics*, Vol. 1, pp. 1-10, https://doi.org/10.1007/s43681-022-00149-5. [216]

Di Geronimo, L. et al. (2020), "UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception", *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1-14, https://doi.org/10.1145/3313831.3376600. [73]

DITP & DGCCRF (2021), *Sciences comportementales appliquées: mieux protéger le consommateur en ligne*. [110]

Drossos, D., M. Zacharioudakis and G. Dionysiou (2019), "Online traffic sources and persuasion techniques: How to change consumer behavior", *ICEEG 2019: Proceedings of the 2019 3rd International Conference on E-commerce, E-Business and E-Government*, pp. 80-84, https://doi.org/10.1145/3340017.3342243. [98]

DSK (2021), *Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021)*. [171]

EC (2022), *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation. Final Report*. [29]

EC (2022), *Consumer Agenda Next steps. Final vote on common actions of priority for 2022*. [233]

EC (2022), *Consumer Agenda Next steps. Other recommendations and conclusions from workshops*. [155]

EC (2021), *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*. [140]

EC (2021), *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*. [162]

EC (2020), *Behavioural Study on Advertising and Marketing Practices in Travel Booking Websites and Apps - Final Report*. [99]

EC (2018), *Behavioural study on advertising and marketing practices in online social media - final report*. [92]

EC (2017), *Study for the Fitness Check of EU consumer and marketing law. Final report*. [186]

EC (2016), *Consumer vulnerability across key markets in the European Union: Final report*. [133]

EC (2016), *Misleading « free » trials and subscription traps for consumers in the EU : final report.*. [71]

ECC Sweden (2017), *Subscription Traps in Europe. EU Study into Public Experiences of Subscription Traps in Six Countries in 2017*. [69]

EDPB (2022), *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them. Version 1.0*. [175]

EDPB (2020), *Guidelines 05/2020 on consent under Regulation 2016/679*. [170]

Egberts, A. (2021), *Manipulation through Design: A Law and Economics Analysis of EU Dark Patterns Regulation*. [50]

EP (2022), *CORRIGENDUM to the position of the European Parliament adopted at first reading on 5 July 2022 with a view to the adoption of Regulation (EU) 2022/... of the European Parliament and of the Council on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)P9_TA(2022)0269 (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD))*. [54]

EP (2022), *P9_TA(2022)0270 Digital Markets Act ***I European Parliament legislative resolution of 5 July 2022 on the proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) (COM(2020)0842 – C9-0419/2020 – 2020/0374(COD)*. [55]

Falbe, T., M. Frederiksen and K. Andersen (2020), *The Ethical Design Handbook*, Smashing Media AG. [210]

Fansher, M., S. Chivukula and C. Gray (2018), “#Darkpatterns: UX Practitioner Conversations About Ethical Design”, *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, https://doi.org/10.1145/3170427.3188553. [205]

Firth, J. et al. (2019), “The “online brain”: how the Internet may be changing our cognition”, *World Psychiatry*, Vol. 18/2, pp. 119-129, https://doi.org/10.1002/wps.20617. [36]

Fletcher, A. et al. (2021), “Consumer Protection for Online Markets and Large Digital Platforms”, *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.3923588. [139]

Forbrukerrådet (2022), *Insert coin: How the gaming industry exploits consumers using loot boxes*. [89]

Forbrukerrådet (2021), *You can log out, but you can never leave*. [86]

Forbrukerrådet (2018), *Deceived by design*. [27]

Forbrukerrådet (2018), *Every step you take*. [83]

Gabaix, X. and D. Laibson (2006), “Shrouded attributes, consumer myopia, and information suppression in competitive markets”, *Quarterly Journal of Economics*, Vol. 121/2, pp. 505-540, https://doi.org/10.1162/qjec.2006.121.2.505. [47]

Goodstein, S. (2021), “When the cat’s away: techlash, loot boxes, and regulating “dark patterns” in the video game industry’s monetization strategies”, *University of Colorado Law Review*, Vol. 92/1. [88]

Graßl, P. et al. (2021), “Dark and Bright Patterns in Cookie Consent Requests”, *Journal of Digital Social Research*, Vol. 3/1, pp. 1-38, https://doi.org/10.33621/jdsr.v3i1.54. [94]

Gray, C. et al. (2021), “End User Accounts of Dark Patterns as Felt Manipulation”, *Proceedings of the ACM on Human-Computer Interaction*, Vol. 5/CSCW2, pp. 1-25, https://doi.org/10.1145/3479516. [119]

Gray, C., S. Chivukula and A. Lee (2020), “What Kind of Work Do ``Asshole Designers’’ Create? Describing Properties of Ethical Concern on Reddit”, https://doi.org/10.1145/3357236.3395486. [209]

Gray, C. et al. (2018), “The dark (patterns) side of UX design”, *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, https://doi.org/10.1145/3173574.3174108. [23]

Gunawan, J., D. Choffnes and C. Wilson (2021), “Towards an Understanding of Dark Pattern Privacy Harms”, *CHI’21, May 8–13, 2021, Online Virtual Conference*. [115]

Gunawan, J. et al. (2021), “A Comparative Study of Dark Patterns across Web and Mobile Modalities”, *Proceedings of the ACM on Human-Computer Interaction*, Vol. 5/CSCW2, pp. 1-29, https://doi.org/10.1145/3479521. [74]

Hanson, J. and D. Kysar (1999), “Taking behavioralism seriously: some evidence of market manipulation”, *Harvard Law Review*, Vol. 112/7, pp. 1422-1570, https://doi.org/10.2307/1342413. [17]

Hartzog, W. (2018), *Privacy’s Blueprint: The Battle to Control the Design of New Technologies*, Harvard University Press. [158]

Hausner, P. and M. Gertz (2021), “Dark Patterns in the Interaction with Cookie Banners”, *CHI Conference on Human Factors in Computing Systems (CHI 2021), May 8-13, 2021*. [199]

Helberger, N. et al. (2021), *EU CONSUMER PROTECTION 2.0 Structural asymmetries in digital consumer markets*. [138]

Himes, J. and J. Crevier (2021), *“Something Is Happening Here but You Don’t Know What It Is. Do You, Mrs. Jones?” Dark Patterns as an Antitrust Violation*, https://www.competitionpolicyinternational.com/something-is-happening-here-but-you-dont-know-what-it-is-do-you-mrs-jones-dark-patterns-as-an-antitrust-violation/. [126]

Hoofnagle, C., W. Hartzog and D. Solove (2019), *The FTC can rise to the privacy challenge, but not without help from Congress*, https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/. [157]

Howells, G., C. Twigg-Flesner and T. Wilhelmsson (2017), *Rethinking EU consumer law*, Routledge, https://doi.org/10.4324/9781315164830. [66]

Huck, S. and B. Wallace (2015), “The impact of price frames on consumer decision making: Experimental evidence”, *working paper*. [229]

Hung, A. (2021), “Keeping Consumers in the Dark: Addressing ’Nagging’ Concerns and Injury”, *Columbia Law Review*, Vol. 121/8, https://doi.org/10.2139/ssrn.3803936. [56]

Hurwitz, J. (2020), "Designing a Pattern, Darkly", *North Carolina Journal of Law & Technology*, Vol. 22/1, p. 57. [61]

ICAS (2022), *Examples of adjudications/actions of advertising self-regulatory bodies relating to dark patterns communicated to the OECD Secretariat*. [231]

ICC (2018), *ICC Advertising and Marketing Communications Code*. [200]

ICO (2020), *Age appropriate design: a code of practice for online services*. [173]

ICPEN (2019), *Internet sweep on the theme "dark nudges"*. [15]

ICPFTA (2022), *Guidance of the Head of the Israel Consumer Protection and Fair Trade Authority. Use of Default Options*, https://www.gov.il/BlobFolder/generalpage/cpfta_about_international_activity/he/docs_legal_Guidance%20-%20Use%20of%20Default%20Options%20-%20Israel%20Consumer%20Protection%20Authority.pdf. [172]

Institute for the Future and Omidyar Network (2018), *Ethical OS*. [213]

Jarovsky, L. (2022), "Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness", *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.4048582. [65]

Jeong, H. and K. Kwon (2012), "The Effectiveness of Two Online Persuasion Claims: Limited Product Availability and Product Popularity", *Journal of Promotion Management*, Vol. 18/1, pp. 83-99, https://doi.org/10.1080/10496491.2012.646221. [100]

Jerath, K., L. Ma and Y. Park (2014), "Consumer Click Behavior at a Search Engine: The Role of Keyword Popularity", *Journal of Marketing Research*, Vol. 51/4, pp. 480-486, https://doi.org/10.1509/jmr.13.0099. [37]

Kahneman, D., P. Slovic and A. Tversky (eds.) (1982), *Judgment under Uncertainty: Heuristics and Biases*, Cambridge University Press, https://doi.org/10.1017/CBO9780511809477. [232]

Kaufman, D. (2021), *Comments at US FTC workshop "Bringing Light to Dark Patterns"*. [145]

Keizer, T. (2017), *Does social proof and scarcity work for opera lovers? A study into the effectiveness of online persuasion cues on consumer responses within the online ticketing store*, https://purl.utwente.nl/essays/71740 (accessed on 21 June 2021). [101]

Kemp, K. (2020), "Concealed data practices and competition law: why privacy matters", *European Competition Journal*, Vol. 16/2-3, pp. 628-672, https://doi.org/10.1080/17441056.2020.1839228. [43]

King, D. and P. Delfabbro (2018), "Predatory monetization schemes in video games (e.g. 'loot boxes') and internet gaming disorder", *Addiction*, Vol. 113/11, pp. 1967-1969, https://doi.org/10.1111/ADD.14286. [117]

King, J. and A. Stephan (2021), "Regulating Privacy Dark Patterns in Practice - Drawing Inspiration from California Privacy Rights Act", *Georgetown Law Technology Review*, Vol. 5/250. [149]

Kinnaird, Z. (2020), *Dark patterns powered by machine learning: an intelligent combination*, https://uxdesign.cc/dark-patterns-powered-by-machine-learning-an-intelligent-combination-f2804ed028ce. [42]

Klein, T. (2021), *Bits of advice: the true colours of dark patterns*, https://www.oxera.com/insights/agenda/articles/bits-of-advice-the-true-colours-of-dark-patterns/. [191]

Kollnig, K., S. Datta and M. Van Kleek (2021), "I Want My App That Way: Reclaiming Sovereignty Over Personal Devices", *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, https://doi.org/10.1145/3411763.3451632. [198]

Konsumentverket (2021), *Barriers to a well-functioning digital market. Effects of visual design and information disclosures on consumer detriment.* [222]

Kozyreva, A., S. Lewandowsky and R. Hertwig (2020), "Citizens Versus the Internet: Confronting Digital Challenges With Cognitive Tools", *Psychological Science in the Public Interest*, Vol. 21/3, pp. 103-156, https://doi.org/10.1177/1529100620946707. [196]

Kristofferson, K. et al. (2017), "The dark side of scarcity promotions: How exposure to limited-quantity promotions can induce aggression", *Journal of Consumer Research*, Vol. 43/5, pp. 683-706, https://doi.org/10.1093/JCR/UCW056. [121]

Leiser, M. (2020), "'Dark Patterns': the case for regulatory pluralism", *SSRN Electronic Journal*, http://dx.doi.org/10.2139/ssrn.3625637. [48]

Loewenstein, G. et al. (2015), "Warning: You are about to be nudged", *Behavioral Science & Policy*, Vol. 1/1, pp. 35-42. [105]

London Economics (2013), *Partitioned Pricing Research. A behavioural experiment*. [227]

Luguri, J. and L. Strahilevitz (2021), "Shining a Light on Dark Patterns", *Journal of Legal Analysis*, Vol. 13/1, pp. 43-109, https://doi.org/10.1093/jla/laaa006. [25]

Luguri, J. and L. Strahilevitz (2019), *Shining a Light on Dark Patterns, draft*. [223]

MacCarthy, M. and K. Propp (2021), *Machines learn that Brussels writes the rules: The EU's new AI regulation*, https://www.brookings.edu/blog/techtank/2021/05/04/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/. [163]

Machuletz, D. and R. Böhme (2019), "Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR", *Proceedings on Privacy Enhancing Technologies*, Vol. 2020/2, pp. 481-498, https://doi.org/10.2478/popets-2020-0037. [93]

Magnusson, J. (2019), *Improving Dark Pattern Literacy of End Users*. [197]

Maier, M. and R. Harr (2020), "Dark design patterns: An end-user perspective", *Human Technology*, Vol. 16/2, pp. 170-199, https://doi.org/10.17011/ht/urn.202008245641. [103]

Mangen, A., B. Walgermo and K. Brønnick (2013), "Reading linear texts on paper versus computer screen: Effects on reading comprehension", *International Journal of Educational Research*, Vol. 58, pp. 61-68, https://doi.org/10.1016/j.ijer.2012.12.002. [38]

Mathur, A. et al. (2019), "Dark patterns at scale: Findings from a crawl of 11K shopping websites", *Proceedings of the ACM on Human-Computer Interaction*, Vol. 3/CSCW, https://doi.org/10.1145/3359183. [24]

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. [53]

Matte, C., N. Bielova and C. Santos (2020), "Do cookie banners respect my choice?: Measuring legal compliance of banners from IAB europe's transparency and consent framework", *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 791-809, https://doi.org/10.1109/SP40000.2020.00076. [78]

McEntaggart, K., J. Etienne and J. Uddin (2019), *Designing self- and co-regulation initiatives: evidence on best practices. A literature review. BEIS Research Paper Number 2019/025*. [220]

Meske, C. and I. Amojo (2020), "Ethical Guidelines for the Construction of Digital Nudges", *53rd Hawaii International Conference on Systems Sciences (HICSS)*, pp. 3928-3937, https://doi.org/10.48550/arXiv.2003.05249. [211]

Meyer, M. et al. (2019), "Advertising in Young Children's Apps: A Content Analysis", *Journal of developmental and behavioral pediatrics*, Vol. 40/1, pp. 32-39, https://doi.org/10.1097/DBP.0000000000000622. [136]

Moran, N. (2020), "Illusion of safety: How consumers underestimate manipulation and deception in online (vs. offline) shopping contexts", *Journal of Consumer Affairs*, Vol. 54/3, pp. 890-911, https://doi.org/10.1111/JOCA.12313. [40]

Morton, F. and D. Dinielli (2020), *Roadmap for an Antitrust Case Against Facebook*. [114]

Moser, C., S. Schoenebeck and P. Resnick (2019), "Impulse buying: Design practices and consumer needs", *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*, https://doi.org/10.1145/3290605.3300472. [75]

NAI (2022), *Best Practices for User Choice and Transparency*. [201]

NAI (2021), *Bringing Dark Patterns to Light: An FTC Workshop. Comments from the Network Advertising Initiative (NAI) filed with the Federal Trade Commission*. [166]

Narayanan, A. et al. (2020), "Dark patterns: Past, Present, and Future. The Evolution of Tricky User Interfaces", *Communications of the ACM*, Vol. 63/9, pp. 42-47, https://doi.org/10.1145/3397884. [34]

Nguyen, S. and J. McNealy (2021), *I, Obscura - Illuminating deceptive design patterns in the wild*. [168]

Nielsen, J. (2020), *10 Usability Heuristics for User Interface Design*, https://www.nngroup.com/articles/ten-usability-heuristics/. [214]

Nouwens, M. et al. (2020), "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence", *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1-13, https://doi.org/10.1145/3313831.3376321. [79]

noyb (2021), *noyb aims to end "cookie banner terror" and issues more than 500 GDPR complaints*, https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints. [81]

OECD (2021), "Implementation toolkit on legislative actions for consumer protection enforcement co-operation", *OECD Digital Economy Papers*, No. 310, OECD Publishing, Paris, https://dx.doi.org/10.1787/eddcdc57-en. [193]

OECD (2021), *Roundtable on Dark Commercial Patterns Online: Summary of discussion*, https://one.oecd.org/document/DSTI/CP/CPS(2020)23/FINAL/en/pdf. [1]

OECD (2021), "The effects of online disclosure about personalised pricing on consumers: Results from a lab experiment in Ireland and Chile", *OECD Digital Economy Papers*, No. 303, OECD Publishing, Paris, https://dx.doi.org/10.1787/1ce1de63-en. [183]

OECD (2020), *Background note - Consumer Data Rights and Competition*. [123]

OECD (2019), *Artificial Intelligence in Society*, OECD Publishing, Paris, https://dx.doi.org/10.1787/eedfee77-en. [9]

OECD (2019), "Good practice guide on consumer data", *OECD Digital Economy Papers*, No. 290, OECD Publishing, Paris, https://dx.doi.org/10.1787/e0040128-en. [2]

OECD (2019), "Good practice guide on online advertising: Protecting consumers in e-commerce", *OECD Digital Economy Papers*, No. 279, OECD Publishing, Paris, https://dx.doi.org/10.1787/9678e5b1-en. [3]

OECD (2019), "Good practice guide on online consumer ratings and reviews", *OECD Digital Economy Papers*, No. 288, OECD Publishing, Paris, https://dx.doi.org/10.1787/0f9362cf-en. [4]

OECD (2019), "Online advertising: Trends, benefits and risks for consumers", *OECD Digital Economy Papers*, No. 272, OECD Publishing, Paris, https://dx.doi.org/10.1787/1f42c85d-en. [5]

OECD (2019), *Tools and Ethics for Applied Behavioural Insights: The BASIC Toolkit*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9ea76a8f-en. [230]

OECD (2018), "Improving online disclosures with behavioural insights", *OECD Digital Economy Papers*, No. 269, OECD Publishing, Paris, https://dx.doi.org/10.1787/39026ff4-en. [6]

OECD (2017), "Use of Behavioural Insights in Consumer Policy", *OECD Science, Technology and Industry Policy Papers*, No. 36, OECD Publishing, Paris, https://dx.doi.org/10.1787/c2203c35-en. [8]

OECD (2016), *OECD Recommendation of the Council on Consumer Protection in E-Commerce*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264255258-en. [234]

OECD (2015), "Industry Self Regulation: Role and Use in Supporting Consumer Interests", *OECD Digital Economy Papers*, No. 247, OECD Publishing, Paris, https://dx.doi.org/10.1787/5js4k1fjqkwh-en. [219]

OECD (2010), *Consumer Policy Toolkit*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264079663-en. [7]

OECD (forthcoming), *Consumer Vulnerability in the Digital Age*. [10]

OECD (forthcoming), *Enhancing Online Disclosure Effectiveness*. [35]

Ohm, P. (2018), "Forthright Code", *Houston Law Review*, Vol. 56/2, pp. 471-504. [154]

Otto, R. (2020), *Autoplay and infinite scroll - If we love our dark patterns are they really dark?*, https://rene-otto.medium.com/autoplay-and-infinite-scroll-8607abe52bb7. [60]

Paterson, J. and E. Bant (2020), "Should Australia Introduce a Prohibition on Unfair Trading? Responding to Exploitative Business Systems in Person and Online", *Journal of Consumer Policy*, Vol. 44/1, pp. 1-19, https://doi.org/10.1007/s10603-020-09467-9. [156]

Paterson, J. et al. (2015), ""Safety Net" Consumer Protection: Using Prohibitions on Unfair and Unconscionable Conduct to Respond to Predatory Business Models", *Journal of Consumer Policy*, Vol. 38, pp. 331-355, https://doi.org/10.1007/S10603-014-9276-Y. [185]

Persson, P. (2018), "Attention manipulation and information overload", *Behavioural Public Policy*, Vol. 2/1, pp. 78-106, https://doi.org/10.1017/bpp.2017.10. [180]

Petticrew, M. et al. (2020), “Dark Nudges and Sludge in Big Alcohol: Behavioral Economics, Cognitive Biases, and Alcohol Industry Corporate Social Responsibility”, *Milbank Quarterly*, Vol. 98/4, pp. 1290-1328, https://doi.org/10.1111/1468-0009.12475. [14]

Plateforme RSE (2020), *Corporate Digital Responsibility. 1. Data: key issues. Synthesis*. [204]

PROFECO (2020), *¡Piénsalo antes de dar clic!*. [195]

Purohit, A., L. Barclay and A. Holzer (2020), “Designing for digital detox: Making social media less addictive with digital nudges”, *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, https://doi.org/10.1145/3334480.3382810. [116]

Radesky, J. (2021), *Comments at US FTC workshop “Bringing light to dark patterns”*. [135]

Radesky, J. et al. (2022), “Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children”, *JAMA Network Open*, Vol. 5/6, p. e2217641, https://doi.org/10.1001/jamanetworkopen.2022.17641. [58]

Rasch, A., M. Thöne and T. Wenzel (2020), “Drip pricing and its regulation: Experimental evidence”, *Journal of Economic Behavior and Organization*, Vol. 176, pp. 353-370, https://doi.org/10.1016/j.jebo.2020.04.007. [122]

Repetto, L. and A. Solís (2020), “The Price of Inattention: Evidence from the Swedish Housing Market”, *Journal of the European Economic Association*, Vol. 18/6, pp. 3261-3304, https://doi.org/10.1093/jeea/jvz065. [63]

Rieger, S. and C. Sinders (2020), *Dark Patterns: Regulating Digital Design. How digital design practices un-dermine public policy efforts & how governments and regulators can respond*. [28]

Rimm, J. (2021), *Comments at US FTC workshop “Bringing Dark Patterns to Light”*. [194]

Robbert, T. and S. Roth (2014), “The flip side of drip pricing”, *Journal of Product & Brand Management*, Vol. 23/6, pp. 413-419, https://doi.org/10.1108/JPBM-06-2014-0638. [130]

Rosca, C. et al. (2021), “Digital monitoring of unlawful dark patterns”, *Paper presented at What can CHI do about dark patterns?, Yokohama, Japan.*. [190]

Santana, S., S. Dallas and V. Morwitz (2020), “Consumer reactions to drip pricing”, *Marketing Science*, Vol. 39/1, pp. 188-210, https://doi.org/10.1287/mksc.2019.1207. [224]

Sarinsky, M. (2021), *Stop the Hidden-Fee Rip-Off*, https://www.nytimes.com/2021/08/02/opinion/consumers-drip-pricing.html. [51]

Schneider, C., M. Weinmann and J. Brocke (2018), “Digital nudging: Guiding online user choices through interface design”, *Communications of the ACM*, Vol. 61/7, pp. 67-73, https://doi.org/10.1145/3213765. [67]

Seizov, O., A. Wulf and J. Luzak (2019), “The Transparent Trap: A Multidisciplinary Perspective on the Design of Transparent Online Disclosures in the EU”, *Journal of Consumer Policy*, Vol. 42/1, pp. 149-173, https://doi.org/10.1007/s10603-018-9393-0. [179]

SERNAC (2022), *Consentimiento En El Uso De Cookies: Evidencia Experimental Sobre El Impacto De La Privacidad Por Defecto Y Los Patrones Oscuros En Las Decisiones De Los Consumidores (Cookie consent: Impact Of Privacy By Default And Dark Patterns on Consumer Decisions)*. [106]

SERNAC (2021), *Informe de resultados de levantamiento de dark patterns en comercio electrónico (Report on the results of a sweep concerning dark patterns in e-commerce).* [72]

Shahab, S. and L. Lades (2021), "Sludge and transaction costs", *Behavioural Public Policy*, pp. 1-22, https://doi.org/10.1017/bpp.2021.12. [127]

Shamonsky, D. (2018), "Developing a Code of Ethics for UX Design: What We Can Learn from the Field of Architecture", *User Experience Magazine*, Vol. 18/4. [208]

Shaw, S. (2019), *Consumers Are Becoming Wise to Your Nudge*, https://behavioralscientist.org/consumers-are-becoming-wise-to-your-nudge/. [120]

Siciliani, P., C. Riefa and H. Gamper (2019), *Consumer Theories of Harm*, Hart Publishing, https://doi.org/10.5040/9781509916887. [132]

Sin, R. et al. (2022), "Dark patterns in online shopping: do they work and can nudges help mitigate impulse buying?", *Behavioural Public Policy*, pp. 1-27, https://doi.org/10.1017/bpp.2022.11. [96]

Slaughter, R. (2021), *Comments at US FTC workshop "Bringing Dark Patterns to Light".* [124]

Soe, T. et al. (2020), "Circumvention by design -- dark patterns in cookie consents for online news outlets", *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, https://doi.org/10.1145/3419249.3420132. [80]

Soman, D. et al. (2019), "Seeing Sludge: Towards a Dashboard to Help Organizations Recognize Impedance to End-User Decisions and Action", *SSRN Electronic Journal*, http://dx.doi.org/10.2139/ssrn.3460734. [217]

Stavrakakis, I. et al. (2021), "A Framework of Web-Based Dark Patterns that can be Detected Manually or Automatically", *International Journal on Advances in Intelligent Systems*, Vol. 14, https://doi.org/10.21427/20G8-D176. [76]

Stemler, A., J. Perry and T. Haugh (2020), "The code of the platform", *Georgia Law Review*, Vol. 54/2, pp. 605-661. [153]

Stigler Committee (2019), *Final Report*. [49]

Strahilevitz, L. (2021), *Comments at US FTC workshop "Bringing Dark Patterns to Light".* [95]

Strahilevitz, L. and J. Luguri (2019), "CONSUMERTARIAN DEFAULT RULES", *Law and Contemporary Problems*, Vol. 82/4, pp. 139-161. [164]

Sunstein, C. (2020), "Sludge Audits", *Behavioural Public Policy*, pp. 1-20, https://doi.org/10.1017/bpp.2019.32. [215]

Sunstein, C. (2016), "Fifty Shades of Manipulation", *J. Behavioral Marketing*, Vol. 213, http://dx.doi.org/10.2139/ssrn.2565892. [64]

Susser, D., B. Roessler and H. Nissenbaum (2019), "Online Manipulation: Hidden Influences in a Digital World", *Georgetown Law Technology Review*, Vol. 4/1, http://dx.doi.org/10.2139/ssrn.3306006. [57]

Susser, D., B. Roessler and H. Nissenbaum (2019), "Technology, autonomy, and manipulation", *Internet Policy Review*, Vol. 8/2, https://doi.org/10.14763/2019.2.1410. [107]

Temby, S. and J. Vasquez (2020), *Regulating the web – is the Australian Consumer Law 'fit for purpose'?*, https://www.maddocks.com.au/insights/regulating-the-web-is-the-australian-consumer-law-fit-for-purpose. [147]

Teubner, T. and A. Graul (2020), "Only one room left! How scarcity cues affect booking intentions on hospitality platforms", *Electronic Commerce Research and Applications*, Vol. 39, p. 100910, https://doi.org/10.1016/J.ELERAP.2019.100910. [97]

Thaler, R. (2018), "Nudge, not sludge", *Science*, Vol. 361/6401, p. 431, https://doi.org/10.1126/science.aau9241. [13]

Thaler, R. (2015), *The Power of Nudges, for Good and Bad*, https://www.nytimes.com/2015/11/01/upshot/the-power-of-nudges-for-good-and-bad.html. [16]

Thaler, R. and C. Sunstein (2008), *Nudge: Improving Decisions About Health, Wealth, and Happiness*, Yale University Press. [12]

Totzek, D. and G. Jurgensen (2021), "Many a little makes a mickle: Why do consumers negatively react to sequential price disclosure?", *Psychology & Marketing*, Vol. 38/1, pp. 113-128, https://doi.org/10.1002/MAR.21426. [131]

Tran, K. (2020), "Partitioned Pricing and Consumer Welfare", *DIW Berlin Discussion Paper* 1888, https://doi.org/10.2139/ssrn.3676900. [225]

UK BEIS (2021), *Reforming Competition and Consumer Policy. Driving growth and delivering competitive markets that work for consumers*. [150]

UK DCMS (2020), *Loot Boxes in Video Games. Call for Evidence*. [90]

US FTC (2022), *Bringing Dark Patterns to Light - Staff Report*. [146]

US FTC (2021), *Enforcement Policy Statement Regarding Negative Option Marketing*. [159]

US FTC (2021), *Transcript of online workshop "Bringing Light to Dark Patterns"*. [221]

US FTC (2017), *ECONOMIC ANALYSIS OF HOTEL RESORT FEES*. [226]

US FTC (1984), *FTC Policy Statement on Deception*. [143]

Utz, C. et al. (2019), "(Un)informed Consent: Studying GDPR consent notices in the field", *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*, pp. 973-990, https://doi.org/10.1145/3319535.3354212. [77]

Van Der Lee, J. et al. (2021), "Ethical design: Persuasion, not deception", *Journal of Digital & Social Media Marketing*, Vol. 9/2, pp. 135-148. [218]

Veltri, G. et al. (2020), "The impact of online platform transparency of information on consumers' choices", *Behavioural Public Policy*, pp. 1-28, https://doi.org/10.1017/bpp.2020.11. [176]

Voigt, C., S. Schlögl and A. Groth (2021), "Dark Patterns in Online Shopping: Of Sneaky Tricks, Perceived Annoyance and Respective Brand Trust", in *HCI in Business, Government and Organizations, Lecture Notes in Computer Science*, Springer International Publishing, Cham, https://doi.org/10.1007/978-3-030-77750-0_10. [118]

VZBV (2021), *Jedes zehnte Cookie-Banner ist klar rechtswidrig*, https://www.vzbv.de/pressemitteilungen/jedes-zehnte-cookie-banner-ist-klar-rechtswidrig. [82]

Waldman, A. (2020), “Cognitive biases, dark patterns, and the ‘privacy paradox’”, *Current Opinion in Psychology*, Vol. 31, pp. 105-109, https://doi.org/10.1016/j.copsyc.2019.08.025. [129]

Warner, M. (2021), *Comments at US FTC workshop “Bringing Dark Patterns to Light”.* [144]

Willis, L. (2020), “Deception by Design”, *Harvard Journal of Law & Technology*, Vol. 34/1, pp. 115-190. [39]

Zagal, J., S. Björk and C. Lewis (2013), “Dark Patterns in the Design of Games”, *FDG*. [30]

Zarsky, T. (2019), “Privacy and manipulation in the digital age”, *Theoretical Inquiries in Law*, Vol. 20/1, pp. 157-158, https://doi.org/10.1515/til-2019-0006. [108]

Zhou, K. (2022), *Design Ethically*, https://www.designethically.com/. [212]

Notes

[1] Although the focus of the report is restricted to dark commercial patterns employed by businesses vis-à-vis consumers (thus excluding e.g. dark patterns of a political nature), the remainder of the report refers to "dark patterns" rather than "dark commercial patterns", for simplicity.

[2] E-commerce in this report refers to business-to-consumer transactions for goods and services conducted online. In line with the 2016 OECD Recommendation on Consumer Protection in E-Commerce, the term covers both monetary and non-monetary transactions (OECD, 2016[239]). Non-monetary transactions often involve digital content products, including software, apps, videos, music, images, e-books, cloud computing, and social networking services, provided "free" in exchange for personal data and/or exposure to advertising. Non-monetary transactions can be part of more complex arrangements in which a basic service is provided free of charge, but "premium" versions with additional features are also offered against a payment ("freemium" models) (OECD, 2019[1]).

[3] According to Kahneman, Slovic and Tversky (1982[231]), heuristics are the "shortcuts" that people use to reduce task complexity in judgment and choice, and biases are the resulting gaps between normative behaviour and the heuristically determined behaviour.

[4] See OECD (2017[7]) for a list of common behavioural biases relevant for consumer policy and a detailed discussion of the use of behavioural insights in consumer policy. See also OECD (2019[229]) for an OECD toolkit providing practitioners and policy makers with a step-by-step process for analysing a policy problem, building strategies, and developing behaviourally informed interventions. See also Mathur et al. (2019[24]), who set out cognitive biases linked to specific dark patterns.

[5] See https://dapde.de/en/dark-patterns-en/types-and-examples-en/hindernisse2-en/ .

[6] It should be noted that some consumer protection authorities have not considered misleading testimonials to be dark patterns as they have addressed them via separate targeted measures. Nonetheless, this report considers misleading testimonials can be considered dark patterns to the extent they meet the working definition set out in Section 2.

[7] Zagal, Björk and Lewis (2013[30]) provided one of the first characterisations of dark patterns in games, defining a "dark game design pattern" as "a pattern used intentionally by a game creator to cause negative experiences for players that are against their best interests and happen without their consent". They considered dark game design patterns fell into three categories based on what the player is being deceived into spending or using – either time, money or social capital. Examples include *grinding* (performing repetitive and tedious tasks), *playing by appointment* (requiring players to play at specific times), *pay to skip* (pay to continue playing), *pre-delivered content* (requiring a fee to access additional content delivered with the game), *monetised rivalries* (encouraging players to spend money to achieve in-game status), and *social pyramid schemes* (encouraging players to invite friends to participate).

[8] See https://www.congress.gov/bill/117th-congress/senate-bill/3330/text. The legislation had not passed at the time of writing.

[9] See https://cppa.ca.gov/meetings/materials/20220608_item3.pdf

[10] See e.g. https://medium.com/@fesja/how-euronet-uses-dark-patterns-to-try-to-deceive-you-670e1dd62dd7

[11] See e.g. https://medium.com/@jochen.t/dark-patterns-what-princeton-university-researchers-got-wrong-cbdffd26520e

[12] "Legitimate practices, for example in advertising, that are in compliance with Union law should not in themselves be regarded as constituting dark patterns" (Recital 67) (EP, 2022[54])

[13] See https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1333

[14] See https://archive.uie.com/brainsparks/2011/09/14/do-users-change-their-settings/

[15] See also the CCP's report on enhancing online disclosure effectiveness (OECD, forthcoming[35]), showing that, in a similar vein, disclosures are at particular risk of being disregarded when consumers do not see an alternative to accepting the disclosed information in order to proceed towards their original goal. The report also highlights consumers may become habituated when they encounter the same or similar online disclosures repeatedly and decide to focus their attention elsewhere.

[16] The Dark Patterns Tip Line presents several concrete examples of dark patterns causing a denial of choice; see https://darkpatternstipline.org/harms/denied-choice/.

[17] The Dark Patterns Tip Line presents a range of concrete examples of such different forms of detriment resulting from certain dark patterns; see https://darkpatternstipline.org/harms.

[18] See https://www.ftc.gov/enforcement/cases-proceedings/172-3186/age-learning-inc-abcmouse .

[19] A quality-adjusted price rises when the monetary price of a service stays constant while either its quality falls or the amount of data required in trade increases (Morton and Dinielli, 2020[115]).

[20] The Dark Patterns Tip Line presents several concrete examples of dark patterns causing consumers to feel shame, feel tricked or waste time; see https://darkpatternstipline.org/harms.

[21] Mathur, Mayer and Kshirsagar (2021[53]) also list price transparency and unintended societal consequences as possible impacts of dark patterns on collective welfare. However, as impacts on price transparency can also be considered intermediate impacts affecting both competition and financial loss, they are not listed separately here. Unintended societal consequences of dark patterns, such as collection of data to feed a political disinformation campaign (Mathur, Kshirsagar and Mayer, 2021[53]), being beyond the realm of consumer welfare in commercial transactions are outside the scope of this report.

[22] See https://ec.europa.eu/commission/presscorner/detail/en/IP_14_847

[23] See https://www.ftc.gov/news-events/press-releases/2014/09/google-refund-consumers-least-19-million-settle-ftc-complaint-it ; https://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million. ; and https://www.ftc.gov/news-events/press-releases/2016/04/federal-court-finds-amazon-liable-billing-parents-childrens

[24] See https://www.propublica.org/article/turbotax-just-tricked-you-into-paying-to-file-your-taxes

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

[26] See https://www.gov.uk/government/consultations/reforming-competition-and-consumer-policy/outcome/reforming-competition-and-consumer-policy-government-response.

[27] Specifically, the text of the DSA provides that "The Commission may issue guidance on the application of paragraph 1 to specific practices, notably:(a) giving more prominence to certain choices when asking the recipient of the service for a decision; (b) repeatedly requesting a recipient of the service to make a choice where such a choice has already been made, especially by presenting a pop-up that interferes with user experience;(c) making the procedure of terminating a service more difficult than subscribing to it." (EP, 2022[54])

[28] See https://www.warner.senate.gov/public/index.cfm/2021/12/lawmakers-reintroduce-bipartisan-bicameral-legislation-to-ban-manipulative-dark-patterns

[29] See https://www.warner.senate.gov/public/index.cfm/2021/12/lawmakers-reintroduce-bipartisan-bicameral-legislation-to-ban-manipulative-dark-patterns

[30] See https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000041608694/

[31] See https://european-consumer-summit-2022.b2match.io/

[32] The ACCC recommended that "in drafting any unfair practices provision in Australia consideration should be given to the appropriate parameters, and that in developing such parameters, it will likely be useful to have regard to the unfair practices provisions in comparable jurisdictions." (ACCC, 2019[84]).

[33] Under 12 U.S.C. § 5531, the US Consumer Financial Protection Bureau may take action against an "abusive" an act or practice, defined as one that "(1) materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service; or (2) takes unreasonable advantage of (A) a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service; (B) the inability of the consumer to protect the interests of the consumer in selecting or using a consumer financial product or service; or (C) the reasonable reliance by the consumer on a covered person to act in the interests of the consumer." See also Hung (2021[56]).

[34] See https://www.dentons.com/en/insights/articles/2020/october/8/the-new-cancelation-link

[35] See https://www.jdsupra.com/legalnews/new-two-click-cancellation-button-4437257/

[36] See https://www.jdsupra.com/legalnews/new-york-implements-automatic-renewal-8746900/

[37] See https://www.gov.uk/government/consultations/reforming-competition-and-consumer-policy/outcome/reforming-competition-and-consumer-policy-government-response.

[38] See https://oag.ca.gov/system/files/attachments/press-docs/CCPA%20March%2015%20Regs.pdf

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

[40] See e.g. https://www.adexchanger.com/privacy/state-privacy-laws-will-spur-action-against-dark-patterns/ .

[41] See https://www.mondaq.com/canada/privacy-protection/1211264/a-canadian-perspective-on-regulating-dark-patterns and https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading

[42] See https://www.hawley.senate.gov/sen-hawley-introduces-legislation-curb-social-media-addiction

[43] See https://cppa.ca.gov/meetings/materials/20220608_item3.pdf . The draft regulations also provide that any method that does not comply with such principles may be considered a dark pattern.

[44] The FTC Enforcement Policy Statement Regarding Negative Option Marketing draws on decisions by US federal courts and the FTC to remind businesses of their obligations under existing laws and puts them on notice that they will face legal action if their sign-up process fails to provide clear, up-front information, obtain consumers' informed consent, and make cancellation easy. The statement singles out dark patterns such as using "information that interferes with, detracts from, contradicts, or otherwise undermines the ability of consumers to read and understand the disclosures, including any information not directly related to the material terms and conditions of any negative option feature." (US FTC, 2021[159]). See https://www.ftc.gov/news-events/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap for more details.

[45] See https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-looks-modernize-its-guidance-preventing-digital-deception

[46] See https://www.ftc.gov/news-events/press-releases/2021/09/ftc-streamlines-investigations-in-eight-enforcement-areas

[47] See https://www.warner.senate.gov/public/index.cfm/2019/4/senators-introduce-bipartisan-legislation-to-ban-manipulative-dark-patterns

[48] See https://www.gov.uk/government/consultations/reforming-competition-and-consumer-policy/outcome/reforming-competition-and-consumer-policy-government-response.

[49] See Recital 18 of the EU UCPD.

[50] The CCP's report on consumer vulnerability in the digital age discusses the appropriateness and adaptability of such standards in the context of emerging digital practices in further detail (OECD, forthcoming[10]).

[51] The EU UCPD provides that the unfairness of a practice shall be assessed by the impact it has on the "average consumer", understood as a "reasonably informed, circumspect, and observant consumer, taking into account social, cultural and linguistic factors". Similarly, the FTC Act in the US considers how a "reasonable consumer" would be affected by allegedly deceptive advertising or marketing (US FTC, 1984[144]), and courts in Australia have applied an "ordinary or reasonable consumer" test when assessing misleading or deceptive conduct (Corones et al., 2016[184]).

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

[53] See https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/05/ico-and-cma-set-out-blueprint-for-cooperation-in-digital-markets/

[54] See https://www.acm.nl/en/about-acm/cooperation/national-cooperation/digital-regulation-cooperation-platform-sdt

[55] See https://www.acma.gov.au/dp-reg-joint-public-statement

[56] See https://www.ftc.gov/system/files/ftc_gov/pdf/Joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf

[57] At the European Consumer Summit 2022, "Training enforcement authorities on dark patterns with national experts" was considered by participants to be one of the top three "joint actions" for the year ahead (EC, 2022[234]).

[58] See https://www.accc.gov.au/media-release/trivago-to-pay-447-million-in-penalties-for-misleading-consumers-over-hotel-room-rates and www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/FCA/2020/16.html

[59] Regarding friend spam, see e.g. the class action law relating to LinkedIn, Perkins et al. v. LinkedIn Corp., 53 F. Supp. 3d 1190 (N.D. Cal. 2014), https://casetext.com/case/perkins-v-linkedin-corp-3 .

[60] However, it is important to recall, as mentioned in Section 3, that differences in recorded prevalence may partly relate to the identification methodology used (e.g. whether it involved manually registering for a product).

[61] See https://www.gov.uk/government/news/7-out-of-10-people-have-experienced-potential-rip-offs-online-worrying-new-cma-research-reveals
and https://www.gob.pe/institucion/indecopi/noticias/595426-cyber-days-indecopi-advierte-que-proveedores-podrian-usar-patrones-oscuros-en-sus-paginas-web-para-influir-en-decisiones-de-compra.

[62] See https://www.darkpatterns.org/hall-of-shame/all and https://twitter.com/darkpatterns

[63] See https://darkpatternstipline.org/, https://dapde.de/en/publikationen-co-en/dark-pattern-melden_de-en/ and https://www.reddit.com/r/darkpatterns/

[64] See https://globalprivacycontrol.org/

[65] See https://addons.mozilla.org/en-US/firefox/addon/consent-o-matic/

[66] See https://www.dataprotectioncontrol.org/

[67] See https://www.truebill.com/

[68] See https://dapde.de/en/project/projektbeschreibung-en/

[69] See https://thenai.org/accountability/code-enforcement/; https://digitaladvertisingalliance.org/principles; https://edaa.eu/what-we-do/european-principles/

[70] See https://www.asa.org.uk/news/shedding-some-light-on-dark-patterns-and-advertising-regulation.html and https://www.asa.org.uk/codes-and-rulings/advertising-codes/non-broadcast-code.html

[71] See https://www.arpp.org/actualite/avec-invenio-arpp-franchit-nouvelle-etape-issue-de-sa-rd-dans-accompagnement-deontologique-de-publicite-digitale/ ; (ICAS, 2022[232]).

[72] For example, in 2014, the Dutch Advertising Code Committee found scarcity claims on Booking.com were misleading, as it was not clear to the average consumer that they only related to the rooms a hotel had made available through Booking.com. In July 2014, this decision was upheld by the Appeals Board. More recently, the NAD has investigated cases of forced registration and disclosure, hidden information/subscription, bait and switch and drip pricing and the CARU has investigated cases of dark patterns in games for children involving intermediate currency and disguised ads or urgency; the French advertising self-regulatory body (AFPP) has investigated countdown timers; the Spanish advertising self-regulatory body (AUTOCONTROL) has investigated hidden information in advertising and drip pricing; and the Brazilian advertising self-regulatory body (CONAR) has investigated bait and switch, limited stock messages, nagging, drip pricing, hidden information, forced disclosure and disguised ads (ICAS, 2022[232]).

[73] See https://uxpa.org/uxpa-code-of-professional-conduct/

[74] See https://www.design.org.au/code-of-ethics/dia-code-of-ethics

[75] See https://www.warner.senate.gov/public/index.cfm/2021/12/lawmakers-reintroduce-bipartisan-bicameral-legislation-to-ban-manipulative-dark-patterns

[76] See https://www.vox.com/the-goods/2018/10/30/18044678/kids-apps-gaming-manipulative-ads-ftc .

[77] See Perkins et al. v. LinkedIn Corp., 53 F. Supp. 3d 1190 (N.D. Cal. 2014), https://casetext.com/case/perkins-v-linkedin-corp-3 , for details.

[78] See https://www.ftc.gov/news-events/press-releases/2014/09/google-refund-consumers-least-19-million-settle-ftc-complaint-it ; https://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million. ; and https://www.ftc.gov/news-events/press-releases/2016/04/federal-court-finds-amazon-liable-billing-parents-childrens

[79] See https://www.ftc.gov/enforcement/cases-proceedings/172-3186/age-learning-inc-abcmouse.

[80] See https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-returns-more-748000-consumers-who-signed-free-internet-auction-kit-hidden-charges .

[81] See https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

[82] See https://en.agcm.it/en/media/press-releases/2018/12/Facebook-fined-10-million-Euros-by-the-ICA-for-unfair-commercial-practices-for-using-its-subscribers%E2%80%99-data-for-commercial-purposes .

[83] See https://www.forbrukerradet.no/side/google-under-investigation-based-on-complaint-by-the-norwegian-consumer-council/

[84] See https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

[85] See https://www.jdsupra.com/legalnews/the-end-of-dark-patterns-in-cookie-5786302/

[86] See https://www.accc.gov.au/media-release/google-misled-consumers-about-the-collection-and-use-of-location-data

[87] See https://noyb.eu/en/noyb-files-422-formal-gdpr-complaints-nerve-wrecking-cookie-banners

[88] See https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance

[89] See https://www.jdsupra.com/legalnews/google-accused-of-using-dark-patterns-9302701/

[90] See https://www.accc.gov.au/media-release/trivago-loses-appeal-after-misleading-consumers-over-hotel-ads.

[91] See https://www.accc.gov.au/media-release/accc-warns-consumers-to-beware-of-subscription-traps

[92] See https://www.ftc.gov/enforcement/cases-proceedings/152-3067/bunzai-media-group-inc-auravie.

[93] See https://en.agcm.it/en/media/press-releases/2016/7/alias-2345

[94] See FTC Charges Online Marketing Scheme with Deceiving Shoppers | Federal Trade Commission.

[95] See https://www.forbrukerradet.no/siste-nytt/amazon-manipulates-customers-to-stay-subscribed/.

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

[97] See https://www.sic.gov.co/node/7030

[98] See Google to Refund Consumers at Least $19 Million to Settle FTC Complaint It Unlawfully Billed Parents for Children’s Unauthorized In-App Charges | Federal Trade Commission; Federal Court Finds Amazon Liable for Billing Parents for Children’s Unauthorized In-App Charges | Federal Trade Commission (ftc.gov).

[99] See https://www.acm.nl/en/publications/publication/13848/ACM-has-fined-World-Ticket-Center-for-displaying-airfares-incorrectly

[100] See https://www.accc.gov.au/media-release/jetstar-and-virgin-to-pay-penalties-for-misleading-drip-pricing-practices

[101] See https://www.accc.gov.au/media-release/court-finds-that-jetstar-and-virgin-australia-engaged-in-misleading-drip-pricing-practices

[102] See https://www.canada.ca/en/competition-bureau/news/2019/06/ticketmaster-to-pay-45-million-to-settle-misleading-pricing-case.html

[103] See FTC Alleges Fuel Card Marketer FleetCor Charged Hundreds of Millions in Hidden Fees | Federal Trade Commission, https://www.ftc.gov/news-events/press-releases/2019/12/ftc-alleges-fuel-card-marketer-fleetcor-charged-hundreds-millions.

[104] See https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1333

[105] See https://ec.europa.eu/commission/presscorner/detail/en/ip_19_3990

[106] See https://ec.europa.eu/commission/presscorner/detail/en/IP_20_156

[107] See https://ec.europa.eu/info/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions/social-media-and-search-engines_en

[108] See https://www.beuc.eu/publications/consumer-groups-file-complaint-against-whatsapp-unfairly-pressuring-users-accept-its/html

[109] See https://ec.europa.eu/commission/presscorner/detail/en/mex_21_2744

[110] See https://www.beuc.eu/publications/beuc-files-complaint-against-tiktok-multiple-eu-consumer-law-breaches/html

[111] See https://www.gov.uk/cma-cases/secondary-ticketing-websites.

[112] See https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2444.

[113] See https://www.accc.gov.au/media-release/viagogo-to-pay-7-million-for-misleading-consumers

[114] See https://www.gov.uk/cma-cases/online-hotel-booking.

[115] See https://www.gvh.hu/en/press_room/press_releases/press-releases-2020/gigantic-fine-imposed-on-booking.com-by-the-gvh

[116] See FTC, Illinois, and Ohio Stop Scheme That Offered 'Free' Credit Scores, Then Charged Consumers for Credit Monitoring Programs They Never Ordered | Federal Trade Commission.

[117] See https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[118] See https://casetext.com/case/fed-trade-commn-v-leadclick-media-llc-1?__cf_chl_jschl_tk__=pmd_JnilXiWnRijBwvwtOHXSul5IfgRtQ8qvA8BTmFX38i4-1630593688-0-gqNtZGzNAlCjcnBszQdl

[119] See Online Dating Service Agrees to Stop Deceptive Use of Fake Profiles | Federal Trade Commission (ftc.gov).

[120] https://www.ftc.gov/enforcement/cases-proceedings/172-3013/match-group-inc

[121] In 2016 a court also originally granted USD 1.27 billion in monetary relief to consumers harmed by the business' practices, however this ruling was subsequently overturned by the US Supreme Court in 2021. See https://www.supremecourt.gov/opinions/20pdf/19-508_l6gn.pdf for details.