Organisation for Economic Co-operation and Development

DSTI/CP(2020)23/FINAL

Unclassified English - Or. English

19 February 2021

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
COMMITTEE ON CONSUMER POLICY

Roundtable on Dark Commercial Patterns Online

Summary of discussion

JT03471473

Foreword

This document provides a summary of a roundtable on ongoing and emerging consumer risks associated with dark commercial patterns online organised as part of the 99th Session (Part 2) of the Committee on Consumer Policy (CCP) on 6 November 2020.

A supporting document circulated at the roundtable, which includes the final agenda, is attached as Annex A.

The paper was approved and declassified by written procedure on 25 January 2021 and prepared for publication by the Secretariat.

Please cite this paper as: OECD (2021), *Roundtable on Dark Commercial Patterns Online: Summary of discussion*, https://one.oecd.org/document/DSTI/CP/CPS(2020)23/FINAL/en/pdf.

Summary of Roundtable on Dark Commercial Patterns Online

Key findings

Available research and investigations indicate that a growing range of "dark commercial patterns" are widespread online. Although there is now no universally agreed definition of the concept, dark commercial patterns are understood by some as user interfaces used by some online businesses to lead consumers into making decisions they would not have otherwise made if fully informed and capable of selecting alternatives (Mathur et al., 2019[1]). Some dark commercial patterns deceive consumers while others covertly manipulate or coerce them into choices that are not in their best interests.

Examples include long-recognised deceptive commercial practices that violate consumer laws, such as drip pricing and subscription traps[1] (to the extent they are facilitated by website design), as well as newer techniques such as scarcity or urgency cues or misdirecting consumers e.g. into consenting to privacy-intrusive settings.

Some researchers (Mathur, Mayer and Kshirsagar, 2021[2]) have distinguished dark commercial patterns from other persuasive marketing techniques by their modification of choice architecture to hamper consumer decision-making, through changes to the decision space or manipulation of information flows, as well as their potential for individual and collective consumer welfare loss. Such online techniques can cause widespread harm particularly when they can be continuously refined through A/B testing and scaled to many consumers at low cost. Online businesses' ability to collect and use vast amounts of consumer data has also raised concerns about consumers' vulnerability to dark commercial patterns that take advantage of biases and behavioural preferences at the individual consumer level.

While most research to date on dark commercial patterns has been conducted by academic researchers, some consumer protection authorities have begun to identify and address dark commercial patterns using a range of tools. These include mystery shopping; replicating the experience of establishing an online business; web-crawling and web-scraping (i.e. using a program or script to automatically browse many websites and extract relevant data); internet sweeps in cooperation with other authorities; and using enforcement powers to require businesses to share internal marketing material or results of internal experiments.

Dark commercial patterns present complex issues for policy makers and enforcement authorities. In addition to the difficulty of defining what practices constitute a dark commercial pattern, there are challenges in determining the resulting harm to consumers and developing appropriate policy and enforcement responses to the various practices.[2] There may even be differences in how to respond to the large number of practices that are considered to be dark commercial patterns (see Annex A, Box 1). For example, authorities might treat "disguised ads," which are generally already viewed as deceptive under consumer laws in most OECD jurisdictions, differently from "confirmshaming," which might present more novel issues of law. Various complementary approaches are being considered in some jurisdictions to mitigate dark commercial patterns, such as: updating existing legislation outlawing deceptive and fraudulent commercial practices in general; developing and promoting guidance on how existing consumer laws are to apply to dark

commercial patterns; implementing bans on specific online commercial practices; conducting business and consumer awareness campaigns; or collaborating with businesses on the development of voluntary standards, for example through the use of business pledges.

Background

On 6 November 2020, as part of its 99th Session (Part 2), the Committee on Consumer Policy (CCP) organised a roundtable to better understand the various types of dark commercial patterns online, how these may harm consumers, any challenges to the enforcement of consumer protection laws, and whether there may be regulatory gaps that require a policy response (the agenda is attached at Annex A.) The event progresses the work of the CCP in understanding ongoing and emerging consumer risks online, and builds on previous CCP work on consumer data (OECD, 2019[3]), online advertising (OECD, 2019[4]; OECD, 2019[5]), online ratings and reviews (OECD, 2019[6]), improving online disclosures with behavioural insights (OECD, 2018[7]), as well as more recent work on measuring the effectiveness of online disclosures.

The following provides a summary of the roundtable, which featured panellists from academia, consumer protection authorities, and a consumer organisation. It begins with an overview of the main themes that emerged from the discussion, including examples and categories of dark commercial patterns and their defining attributes; evidence of their prevalence online on business' websites or apps; consumer vulnerability; as well as the tools and approaches available to consumer protection authorities and policy makers to identify and mitigate them. It then provides details of the presentations by each of the panellists, before concluding with suggested next steps.

Main themes

What are dark commercial patterns online?

There is as yet no clear or consensus definition of the term "dark commercial patterns," which has been applied to a wide range of online commercial practices (Mathur, Mayer and Kshirsagar, 2021[2]). According to one definition, dark commercial patterns are user interfaces used by some online businesses to lead consumers into making decisions that they would not have otherwise made if fully informed and capable of selecting alternatives (Mathur et al., 2019[1]). Some dark commercial patterns deceive users while others covertly manipulate or coerce them into choices that are not in their best interests. Using a mixture of behavioural nudges and user interface-based techniques honed through A/B testing, dark commercial patterns can often lead consumers to do something - such as spend more money or time on a website or consent to tracking - that is inconsistent with their informed preferences.[3] Examples include use of default settings to, for instance, sneak an additional item into a consumer's basket without consent (e.g. via a checkbox on a prior page); add new and potentially significant charges when a consumer is just about to complete a purchase; or automatically renew an original purchase (e.g. through a hidden subscription trap). Other examples include use of pressure selling, urgency and scarcity cues, misdirection, social proof or obstruction in order to adversely influence consumer decision-making. There have been various attempts to categorise them into broader groupings of patterns with similar characteristics. For a more detailed list of examples and taxonomies, see Box 1 in Annex A, as well as Brignull (2019[8]), Gray et al. (2018[9]) and Mathur et al. (2019[1]).

App or website interface designs that steer consumers into consenting to adverse terms of service or privacy-intrusive settings, e.g. by requiring consumers to opt out of (potentially hidden) default settings or presenting acceptance of an unfavourable option as the default, may also constitute dark commercial patterns. Research shows that, unbeknownst to consumers, such practices often result in the sharing of consumer data with a large number of third parties, including data brokers (Norwegian Consumer Council, 2020[10]). In these circumstances, and especially when combined with long and complicated terms of service and privacy policies,[4] dark commercial patterns may make it more difficult for consumers to give truly informed consent to the use of their data.

Distinguishing dark commercial patterns from other marketing techniques

Two criteria proposed by Mathur, Mayer and Kshirsagar (2021[2]) could be used to distinguish a dark commercial pattern from other marketing techniques, which can also often involve an element of persuasion that plays on human psychological frailties. First, a dark commercial pattern modifies the consumer choice architecture, through a range of possible design attributes that either modify the decision space (i.e. the choices available to the consumer) or manipulate information flows to the consumer, in order to make it especially hard for consumers to make independent and informed decisions. Second, the consumer detriment resulting from dark commercial patterns can involve losses to individual welfare (e.g. financial loss, breach of privacy, or unnecessary cognitive burden when making choices), collective welfare (e.g. reduced competition or loss of trust in online businesses), and individual autonomy (through a reduced ability to make free and fully informed decisions); measuring the extent of such impacts could help determine if a particular commercial practice "crosses the line" (Mathur, Mayer and Kshirsagar, 2021[2]). Moreover, such online techniques have the potential to cause widespread harm particularly when they can be continuously refined through A/B testing and scaled to many consumers at low cost.

How widespread is the problem?

In a sweep conducted in 2019 by the International Consumer Protection Enforcement Network (ICPEN) of 1760 websites/applications of retail businesses across a range of sectors, 429 (24%) were flagged for potential 'dark behavioural nudges'. The top three dark nudge practices identified were pressure selling (e.g. using scarcity claims), drip pricing, and design issues such as obscuring terms and conditions. Another study conducted in 2019 by academic researchers from Princeton University in the United States identified 1,818 instances of dark commercial patterns (falling into 15 categories) in a crawl of around 11,000 websites of retail businesses and online marketplaces (Mathur et al., 2019[1]).[5] Such patterns have also been identified on social media platforms and other websites as a means to promote fraudulent advertising directing consumers to counterfeit and other types of illicit products (TRACIT & AAFA, 2020[11]).

Dark commercial patterns exacerbate the effects of consumers' biases and vulnerabilities

The 2014 OECD Recommendation on Consumer Policy Decision-making (OECD, 2014[12]) defines vulnerable consumers as consumers "who are susceptible to detriment at a particular point in time, owing to the characteristics of the market for a particular product, the product's qualities, the nature of a transaction or the consumer's attributes or circumstances" and disadvantaged consumers as consumers "whose attributes or circumstances are such that they are susceptible to detriment on a persistent basis".[6]

To the extent that dark commercial patterns can be designed to prey specifically on certain behavioural biases, they may be more effective than other techniques in exploiting consumers' vulnerabilities. Although there is no conclusive research on this topic, as is the case for other fraudulent and deceptive marketing techniques, such patterns may disproportionately affect certain types of vulnerable consumers such as less educated or low-income consumers, the elderly or children, consumers who are less proficient with technologies or the language used by the online business, consumers with a cognitive disability but also those who may not typically be regarded as vulnerable, such as gig-economy workers.[7] Furthermore, online businesses are also able to collect vast amounts of consumer data allowing them to better target their marketing techniques, through consumer profiling and potentially combined with AI, in order to maximise conversion rates and sales. They may thereby be able to leverage such data to trigger consumers' personal biases at times, rendering consumers vulnerable in certain contexts.[8]

Various consumer protection authorities [9] are currently conducting further work on consumer vulnerability resulting from the digital transformation, including dark commercial patterns.

What are possible policy and enforcement responses?

Dark commercial patterns present complex issues for policy makers and enforcement authorities. In addition to the difficulty of defining what practices constitute a dark commercial pattern, there are challenges in determining the harm to consumers and developing the appropriate policy and enforcement response to the various practices. There may even be differences in how to respond to the large number of practices that are considered to be dark commercial patterns (see Annex A, Box 1). For example, authorities might treat "disguised ads," which are generally already viewed as deceptive under consumer laws in most OECD jurisdictions, differently from "confirmshaming," which might present more novel issues of law.

Although most research on dark commercial patterns to date has been led by academics, consumer protection authorities can use a range of tools to identify and address dark commercial patterns. These include mystery shopping to replicate the consumer's experience on online businesses' websites and in so doing identify dark commercial patterns. Consumer protection authorities may also seek to replicate the experience of setting up an online business and assessing the availability of apps from third-party entities that generate dark commercial patterns. The individual and personalised nature of dark commercial patterns, however, may make drawing general conclusions about them through mystery shopping difficult, even if segmenting the consumer base may yield general insights for different types of consumers. At a larger scale, consumer protection authorities could also consider internet sweeps for dark commercial patterns, possibly in cooperation with other authorities in the same vein as the 2019 ICPEN sweep of dark nudges.

Checking individual websites can be time-consuming, particularly where there is a need to document several dark commercial patterns on a website or the online consumer journey with screenshots. Authorities could use a web-crawling and scraping (data extraction) tool, such as that employed by some academic researchers (Mathur et al., 2019[1]), to check thousands of websites automatically, including relevant blogs or forums to identify complaints, which could potentially incorporate a machine-learning ability. Developing such tools can be resource-intensive, however, so consumer protection authorities may wish to cooperate with each other or with academia in developing them. Notably, open-source code for web-crawling tools would help foster collaboration.

Consumer protection authorities with robust investigative powers could seek to obtain internal marketing material and the results of businesses' empirical experiments such as A/B testing in investigations and enforcement matters.[10] They may therefore consider requiring businesses to share with them such internal marketing material, to the extent they have appropriate powers and subject to intellectual property considerations, for analysis by digital forensics teams and outside experts. When an authority does not have the authority to obtain such material, it may nonetheless seek to liaise with businesses to better understand the marketing techniques employed.

Such tools and others could also be used to inform broader research, as was done by the UK's Competition & Markets Authority (CMA), which recently completed a market study on online platforms and digital advertising (Competition & Markets Authority, 2020[13]).[11] The study found that online platforms' choice architecture could inhibit consumers' ability to exercise informed choices. This included default settings which favour the platform; long and complex privacy policies and terms, as well as the presentation of information and choices in ways that could 'nudge' consumers to make decisions most favourable to the platforms.

Most OECD jurisdictions already have general consumer protection laws that cover many of the techniques associated with dark commercial patterns that authorities can use to combat the most deceptive practices. Indeed, a number of consumer protection authorities have brought enforcement actions covering practices such as "hidden costs," "misdirection," "subscription traps," and "roach motels," but may not have characterised them as dark commercial patterns. For example, the CMA launched enforcement action against several online hotel booking sites for use of a number of practices on their websites that it believed broke consumer law. This led to the sites making formal commitments to change their practices, including e.g. more transparency around and substantiation of scarcity claims (Competition & Markets Authority, 2019[14]). Proper enforcement of relevant consumer law combined with appropriate penalties are therefore critical to combatting dark commercial patterns. Indeed more competition alone may not suffice to address dark commercial patterns, whose increased prevalence may, according to some researchers, drive some businesses to use them just to stay in business.[12]

Privacy data protection laws could also be enforced against dark commercial patterns that preclude consumers from providing express informed consent to the collection and sharing of information. The EU's General Data Protection Regulation (GDPR), for example, covers practices involving use of consumer data without obtaining freely given, specific, informed and unambiguous consent from consumers.[13]

Apart from enforcement, as in many other emerging areas of consumer law, consumer protection authorities can also develop guidance for businesses on how existing consumer laws apply to dark commercial patterns. The Netherlands Authority for Consumers & Markets (ACM), for example, recently issued guidance for businesses and other market participants on how it applies consumer law to a wide range of online persuasion techniques, including dark commercial patterns, that are commonly used in online choice architectures (Netherlands Authority for Consumers & Markets, 2020[15]). It indicates the ACM's views on the extent to which businesses are permitted to persuade consumers in their decisions through practical examples and explanations. Similarly, considering many consumers are still unaware of the prevalence and danger of dark commercial patterns, consumer protection authorities also have an important role to play in raising awareness and educating businesses and consumers, particularly as new dark commercial patterns are constantly emerging.

Some jurisdictions have considered, as a complement to general consumer protections, legislating bans on specific online commercial practices (which they may consider to be dark commercial patterns) or requiring regulators to establish specific standards in relation to those practices. This could take the form of a blacklist, which would provide clarity to both consumer authorities and businesses on which practices are prohibited. The EU's Unfair Commercial Practices Directive (UCPD), for example, contains a blacklist of commercial practices which are in all circumstances considered unfair. Some dark commercial patterns have been considered to fall within the scope of the UCPD blacklist as well as other existing bans on specific commercial practices.[14]

However, legislating can be as lengthy as litigating. New dark practices may emerge by the time existing ones are banned, and some may only need to be tweaked slightly to fall outside the scope of a ban. An alternative or complementary route to legislation may for businesses and other stakeholders to develop voluntary standards or best practices, including, in some countries, in collaboration with consumer protection authorities. The Corporate Digital Responsibility initiative of the German Federal Ministry of Justice and Consumer Protection, for example, seeks to encourage businesses to go beyond minimum statutory requirements and provide digital services in accordance with key societal values such as fairness, trust and transparency.[15]

Academic perspectives

The roundtable began with a presentation from **Mr. Arunesh Mathur**, researcher at the Center for Information Technology Policy at Princeton University. He first shared his understanding of dark commercial patterns online as "user interface design choices that benefit an online service by leading users into making decisions that – if fully informed and capable of selecting alternatives – they might not make." He discussed different ways of categorising dark commercial patterns, and presented a list of examples identified in Brignull (2019[8]) (see Box 1 in Annex A) as well as well broader groupings of dark commercial patterns identified in Gray et al. (2018[9])(nagging, obstruction, sneaking, interface interference and forced action). He pointed to a recent study he co-authored (Mathur et al., 2019[1]), which through a crawl of around 11,000 shopping websites identified 1,818 instances of dark commercial patterns and categorised them into 15 types.

Mr. Mathur proposed two criteria that could be used to distinguish dark commercial patterns from other marketing techniques based on work in progress at the time (Mathur, Mayer and Kshirsagar, 2021[2]), i.e. the commercial practice in question:

- features specific design attributes, qualified either as asymmetric, covert, restrictive, having disparate impact, deceptive, or hiding information, which aim to modify choice architecture through either modifications to the decision space or manipulation of information flows to the user; and
- leads to negative impacts on individual welfare (financial/privacy/cognitive burden), collective welfare (competition/trust), and individual autonomy. Mr. Mathur suggested that measuring the extent of such impacts could help determine whether the practice "crosses the line".

ICPEN perspectives

Mr. Jean-Pierre Bornais, ICPEN Project Manager and Assistant Deputy Commissioner of the Competition Bureau of Canada (current President of ICPEN), then presented the

results of a 2019 ICPEN sweep on "dark nudges" aimed at identifying possible practices to tackle in jurisdictions and options for joint actions. The sweep occurred over a week in April 2019, covering a wide range of practices and areas such as travel, retail/online shopping, ticket sales, antivirus subscriptions, telecommunications/electronic communications, car rentals, and online gambling. Participating consumer agencies were free to choose the practices and areas to focus on.

In total, 1760 websites/applications of businesses across a range of sectors were searched, of which 429 (24%) were flagged for potential 'dark nudge' problematic conduct. The top three dark nudge practices identified were pressure selling (e.g. using scarcity claims, queues, countdown times, social proof, 'limited price' claims), drip pricing (incremental additions of charges through the purchase process), and design issues (e.g. obscuring important information such as terms and conditions; pre-ticked boxes). Others related to complex promotions (e.g. offering an unlimited service that is not really unlimited); discount claims (e.g. fake reference prices or offers that run more or less permanently); contract and cancellation issues (e.g. no option to cancel/auto rollover; no refunds); privacy and use of consumer data (e.g. consent not requested; need to provide personal data before obtaining terms and conditions). Pressure selling as well as contract renewal terms and general unclear terms and conditions leading to subscription traps were commonly identified by ICPEN members as main areas of concern across sectors. As a follow-up to the sweep, ICPEN members recognised the need for developing guidance to businesses on what a consumer-friendly website looks like as well as awareness campaigns to educate consumers on such practices.

Consumer protection authority and consumer organisation perspectives

Next, **Mr. Dries Cuijpers**, Senior Enforcement Official at the Netherlands Authority for Consumers & Markets (ACM), presented information drawing on the ACM's 2020 guidelines on protecting online consumers (Netherlands Authority for Consumers & Markets, 2020[15]). The guidelines were developed in light of the greater consumer risks posed by increasingly targeted online marketing resulting from businesses' ability to collect significant amounts of consumer data, and to scale them to many consumers at low cost. Covid-19 has furthermore amplified risks by increasing the number of consumers shopping online. The guidelines therefore aim to make explicit the boundaries of online persuasion, by clarifying to businesses how the ACM is applying the EU's UCPD to such marketing techniques. The guidelines provide clear norms on the most common online persuasive techniques and provide examples of what may and may not be permitted.

The ACM has promoted the guidelines through online marketing conferences, talks with businesses, blogs, interviews and social media and consumer education initiatives and has ongoing cases on many of the topics from the guidelines. Mr. Cuijpers noted that the guidelines have facilitated discussions among retailers and online marketing companies on the legality of online commercial practices and shed light on the often excessive focus on conversions at the expense of consumer law compliance. He identified several follow-up topics for policy makers to consider, including whether the proxy by which a marketing technique is assessed in the UCPD, the average consumer, continues to be appropriate in the online world, where marketing is increasingly personalised and most consumers could potentially be considered vulnerable.

Mr. Finn Lützow-Holm Myrstad, Director of Digital Policy at the non-governmental consumer organisation, the Norwegian Consumer Council (NCC), subsequently presented research drawing on the NCC's reports regarding dark commercial patterns and platform

privacy settings (Norwegian Consumer Council, 2018[16]; Norwegian Consumer Council, 2018[17]). He first showed an example of a dark commercial pattern involving a Norwegian airline's website design misdirecting consumers into either rebooking their trip or choosing a voucher, instead of a refund, when faced with a Covid-19-related delayed or cancelled flight. He then described how the NCC uncovered a number of dark commercial patterns when checking mechanisms put in place by Facebook, Google and Microsoft to reflect requirements of the EU's GDPR in 2018 regarding consent to use of personal data. For example, the NCC found that Facebook was using a deceptive app design that nudged consumers into accepting the use of its facial recognition feature. In particular, the app did not provide a clear button to deny consent (misdirection), listed only the benefits of the feature and the risks of not using it ("confirmshaming"), and persistently notified the consumer to review data settings (urgency cues).

Mr. Finn Lützow-Holm Myrstad further pointed to a deceptive click flow used by Google to nudge consumers to consent to location tracking through successive screens displaying a 'next' button with a final screen displaying only an 'agree' button. He also highlighted a hidden default setting, whereby tracking of web and app activity was turned on by default in Google's privacy settings. On the basis of this evidence, the NCC, together with consumer groups from eight other countries, filed a complaint (pending at the time of the roundtable) to the Norwegian Data Protection Authority (Datatilsynet) against Google. They argued that Google was in breach of the GDPR's consent requirements on the basis that consent is neither freely given, specific, informed nor unambiguous.

Finally, **Ms. Mai Webber**, Senior Behavioural Insights & Strategy Advisor at the United Kingdom's Competition & Markets Authority (CMA), presented several examples of tackling dark commercial patterns in the United Kingdom. She indicated that in 2019, the CMA's investigation (Competition & Markets Authority, 2019[14]) into major hotel booking sites identified four main types of dark commercial pattern: hidden charges, misleading discount claims, incorrect reference pricing, and pressure selling techniques, such as scarcity claims. Six hotel booking sites have since made formal commitments to the CMA to change their practices, with resulting benefits to consumers estimated at £34 million. The CMA has also issued principles to guide hotel booking sites (Competition & Markets Authority, 2019[18]). Furthermore, the CMA investigated a ticket reseller, viagogo, for its use of various pressure selling techniques and pricing obfuscation, which subsequently resulted in a court order obliging the company to change its practices.[16] The CMA also explored new techniques to identify dark commercial patterns online, including replicating the experience of setting up an online store to identify website apps that generate dark commercial patterns, or web scraping of online gamers' blogs and forums to identify complaints about dark commercial patterns.

Ms. Webber however highlighted some key challenges to addressing dark commercial patterns. She first noted that more competition alone may not suffice to address dark commercial patterns, whose increased prevalence may drive other businesses to use them to stay in business. She further indicated that dark commercial patterns using 'dynamic defaults', i.e. pre-selected defaults (such as settings or purchases) that are automatically renewed unbeknown to the consumer (Ericson, 2020[19]), may be particularly challenging to address. She suggested that, as with Covid-19, tackling dark commercial patterns should involve a combination of scanning for new threats, early identification and diagnosis, deterrence, user centric interventions, compliance with remedies, and international cooperation.

Next steps

To further develop the CCP's work in relation to dark commercial patterns online over the 2021-22 biennium, the Secretariat (Brigitte Acoca) proposed that the committee develop a background report providing an overview of existing academic and policy literature on the types of dark commercial patterns being used by online businesses, research on their effects on consumer decision-making, as well as policy and enforcement responses implemented in jurisdictions so far. The report could also link to related work to be conducted by the CCP over the 2021-2022 biennium, such as on disclosure effectiveness and artificial intelligence, as well as work by other OECD committees, e.g. regarding privacy or competition.

The Secretariat proposed that once the work is more advanced, the CCP could consider undertaking a behavioural experiment in this area, e.g. a randomised control trial to determine the effect of different patterns on consumer decisions. The Secretariat also suggested that the CCP could consider, at a later stage, an awareness campaign regarding dark commercial patterns, similar to the annual campaigns run by the Working Party on Consumer Product Safety (WPCPS), and possibly in partnership with ICPEN.

Finally, the Secretariat also invited interested delegates to join a new CCP advisory group to help develop the work. Delegates were requested to provide feedback on the proposed next steps and ways to scope out the work for the next biennium on the CCP Community site by 27 November 2020.

Annex A. Supporting document for roundtable on dark commercial patterns online

Purpose

There is growing awareness of "dark patterns" being used by e-commerce businesses in the design of their websites and applications to coerce, steer, or deceive consumers into making unintended and potentially harmful decisions online (Mathur et al., 2019[1]; Brignull, 2019[20]).

The purpose of this roundtable is to better understand the various types of dark patterns, how these may harm consumers, any challenges to the enforcement of consumer protection laws, and whether there may be regulatory gaps that require a policy response.

Background

There have been several attempts to categorise the types of dark patterns that are observed on websites and applications (see Box 1). Many of these take advantage of behavioural biases, such as framing and anchoring, status quo biases, and the endowment effect, to lead consumers into making decisions that may not be in their best interests.

A recent study by Mathur et al. (2019[1]) looked at 53 000 product pages from 11 000 shopping websites, and found 1 818 instances of dark patterns used on 1 254 websites. It further identified 234 instances of deceptive dark patterns on 183 websites and 22 third-party entities that provide shopping websites with the ability to create and implement dark patterns on their sites. The study found that:

> *… the majority* [of dark patterns] *are covert, deceptive, and information hiding in nature. Further, many patterns exploit cognitive biases, such as the default and framing effects.*

Several consumer authorities have also examined how websites and applications may be designed to exploit consumers' behavioural biases. In 2018, the Consumer Authority of Norway studied privacy settings in Facebook, Google and Windows 10 and found that default settings and "dark patterns" in interface design nudged users of these platforms towards more data-intrusive settings (Norwegian Consumer Council, 2018[17]). The Netherlands Authority for Consumers and Markets (ACM) is currently consulting on draft guidelines that outline the extent to which businesses are permitted to nudge consumers in their decisions online and how the ACM will apply consumer law to common persuasion techniques online (Netherlands Authority for Consumers & Markets, 2020[15]).

Some consumer agencies have also taken enforcement action against the use of dark patterns by businesses. For example, the UK's Consumer and Markets Authority (CMA) has an ongoing investigation into the practices of online hotel booking companies (Competition & Markets Authority, 2019[14]). Among other things, six online hotel booking sites have provided formal commitments to the CMA to change practices on their websites that the CMA considers may be misleading consumers. The CMA has also issued *Principles for businesses offering online accommodation booking services* regarding:

- Disclosure about the effect of payments on search results: if such payments affect how search results are ranked, the hotel booking website must explain this to the consumer in clear and prominent static text.
- Pricing: the price shown should be the total cost including compulsory taxes, charges and fees that are reasonably calculable based on the search criteria. Any reference prices should not be misleading in any way.

- Popularity and availability statements: statements about popularity and availability must (i) be clear; (ii) disclose the assumptions, limitations and qualifications that are relevant to the statement; and (iii) be substantiated.

Box 1. Examples of dark commercial patterns

Sneak into basket: the site sneaks an additional item into the consumer's basket without consent, perhaps through an opt-out radio button or a checkbox on a prior page.

Bait and switch: a consumer sets out do something, but instead a different undesirable outcome occurs

Hidden costs: new, additional, and often unusually high charges are added just before a consumer is about to complete a purchase.

Hidden subscription: the consumer incurs a recurring fee under the pretence of a one-time fee or a free trial period. Also called "forced continuity" or subscription traps.

Scarcity and urgency cues: are used to indicate that the good, service or offer will soon run out, perhaps through the use of an imposed deadline on a sale or deal (e.g. by using a countdown timer), low stock messages or high demand messages.

Misdirection: uses visuals, language, and emotion to steer users toward or away from making a particular choice.

"Confirmshaming": methods to guilt the consumer into opting into something. The option to decline is worded in such a way as to shame the user into compliance.

Trick questions: when filling in a form or answering questions, a consumer may be tricked into giving an answer she didn't intend. Upon a quick skim, the question appears to ask one thing, but when read carefully it asks another thing entirely.

Pressured selling: defaults or high-pressure tactics that steer consumers into purchasing a more expensive version of a product (upselling) or related products (cross-selling).

Activity notifications: transient, often recurring and attention grabbing messages that indicate the activity of other users.

Testimonials of uncertain origin: customer testimonials whose origin is not clear.

Roach motel: a consumer gets into a situation very easily, but then finds it is hard to get out of it (e.g. a premium subscription).

Price comparison prevention: the retailer makes it hard for the consumer to compare the price of an item with another item, so she cannot make an informed decision.

Disguised ads: adverts that are disguised as other kinds of content or navigation, in order to get consumers to click on them.

Friend spam: the business asks for the consumer's email or social media permissions under the pretence it will be used for a desirable outcome (e.g. finding friends), but then spams all her contacts in a message that claims to be from her.

Source: Brignull (2019[8]); Mathur et al. (2019[1])

Roundtable agenda

The roundtable will explore ongoing and emerging consumer issues associated with "dark patterns" that are used by some businesses online to coerce, steer, or deceive consumers into making unintended and potentially harmful decisions. The discussion will be preceded by short presentations on the topic from:

- **Mr. Arunesh Mathur**, Center for Information Technology Policy at Princeton University

- **Mr. Jean-Pierre Bornais**, ICPEN Project Manager and Assistant Deputy Commissioner of the Competition Bureau of Canada - President of the International Consumer Protection and Enforcement Network (ICPEN) drawing on the 2019 ICPEN sweep on "dark nudges"
- **Mr. Dries Cuijpers**, Senior Enforcement Official from The Netherlands Authority for Consumers & Markets drawing on the ACM's recent Guidelines on Protection of the online consumer: boundaries of online persuasion
- **Mr. Finn Lützow-Holm Myrstad**, Director of Digital Policy, Norwegian Consumer Council drawing on the NCC's Deceived by Design report regarding dark patterns and platform privacy settings.
- **Ms. Mai Webber,** Senior Behavioural Insights & Strategy Advisor, The United Kingdom Competition & Markets Authority who will discuss several examples of tackling dark patterns in the United Kingdom.

Following each presentation there will be a brief opportunity for delegates to pose short questions to each speaker. Delegates will then be invited to intervene briefly (no more than two minutes) to share experiences from their jurisdictions in response to the questions listed below and roundtable presenters will be asked to comment.

Delegates wishing to make an intervention are encouraged to contact the Secretariat in advance of the session. The Chair and Secretariat will make efforts to accommodate as many interventions as possible based on the time available.

Questions and discussion

Discussion questions (20 minutes)

1. What sort of "dark patterns" online have been identified in jurisdictions? How do they harm consumers?
2. How have consumer authorities addressed those "dark patterns"? What kind of challenges have authorities encountered in their investigations or application of their consumer protection frameworks?
3. Have any regulatory gaps been identified by consumer authorities in addressing any such "dark patterns"? If so, what policy responses are consumer authorities considering?

References

Brignull, H. (2019), *Dark Patterns*, https://www.darkpatterns.org/. [20]

Brignull, H. (2019), *Types of Dark Pattern*, https://www.darkpatterns.org/types-of-dark-pattern. [8]

Calo, R. and A. Rosenblat (2017), "The taking economy: Uber, information, and power", *Columbia Law Review*, Vol. 117/6, pp. 1623-1690, http://dx.doi.org/10.2139/ssrn.2929643. [22]

Competition & Markets Authority (2020), *Online platforms and digital advertising market study*, https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study. [13]

Competition & Markets Authority (2019), *Online hotel booking*, https://www.gov.uk/cma-cases/online-hotel-booking. [14]

Competition & Markets Authority (2019), *Principles for businesses offering online accommodation*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781624/webteam_online_booking_services_principles.pdf. [18]

Ericson, K. (2020), "When consumers do not make an active decision: Dynamic default rules and their equilibrium effects", *Games and Economic Behavior*, Vol. 124, pp. 369-385, http://dx.doi.org/10.1016/j.geb.2020.08.007. [19]

European Commission (2019), *Challenges for consumer protection in digital markets*, http://eitlab.eu/wp-content/uploads/2019/05/Dark-patterns-27-april-2019-AF-Consumer-challenges-in-digital-markets-ppt.pdf. [24]

Gray, C. et al. (2018), *The dark (patterns) side of UX design*, Association for Computing Machinery, http://dx.doi.org/10.1145/3173574.3174108. [9]

Helberger, N. et al. (forthcoming), *Digital Vulnerability & Digital Asymmetry in the Directive 2005/29/EC on unfair commercial practices*. [21]

Mathur, A. et al. (2019), "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites", *Proc. ACM Hum.-Comput. Interact. 3, CSCW*, Vol. November/Article 81, p. 32, http://dx.doi.org/10.1145/3359183. [1]

Mathur, A., J. Mayer and M. Kshirsagar (2021), "What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods", http://dx.doi.org/10.1145/3411764.3445610. [2]

Netherlands Authority for Consumers & Markets (2020), *ACM Guidelines on the Protection of the Online Consumer – Boundaries of online persuasion*, https://www.acm.nl/sites/default/files/documents/2020-02/acm-guidelines-on-the-protection-of-the-online-consumer.pdf. [15]

Norwegian Consumer Council (2020), *Out of Control: How consumers are exploited by the online advertising industry*, https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf. [10]

Norwegian Consumer Council (2018), *Deceived by Design: How tech companies use dark patterns to discourage us from exercising our right to privacy,*, https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf. [17]

Norwegian Consumer Council (2018), *Every Step You Take: How deceptive design lets Google track users 24/7*, https://fil.forbrukerradet.no/wp-content/uploads/2018/11/27-11-18-every-step-you-take.pdf. [16]

OECD (2021), *Joint CCP and WPCPS Going Digital policy note: The role of online marketplaces in enhancing consumer protection*, https://one.oecd.org/document/DSTI/CP(2020)9/FINAL. [26]

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. [3]

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. [4]

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. [6]

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 (2018), "Improving online disclosures with behavioural insights", *OECD Digital Economy Papers*, No. 269, OECD Publishing, Paris, https://dx.doi.org/10.1787/39026ff4-en. [7]

OECD (2016), *OECD Recommendation of the Council on Consumer Protection in E-Commerce*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264255258-en. [25]

OECD (2014), *Recommendation of the Council on Consumer Policy Decision Making*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0403. [12]

OECD (2010), *Consumer Policy Toolkit*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264079663-en. [23]

Scott Morton, F. et al. (2019), *Committee for the Study of Digital Platforms Market Structure and Antitrust Subcommittee Report*. [27]

TRACIT & AAFA (2020), *Fraudulent Advertising Online: Emerging Risks and Consumer Fraud*, https://www.tracit.org/uploads/1/0/2/2/102238034/tracit_fraudulentadvertisingonline_july21_2020_final.pdf. [11]

Notes

[1] The OECD E-commerce Recommendation, for example, recommends that businesses should ensure that advertised prices do not misrepresent or hide the total cost of a good or a service, and that they should not misrepresent or hide terms and conditions that are likely to affect a consumer's decision regarding a transaction (OECD, 2016[25]).

[2] The OECD Consumer Policy Toolkit provides a standard model for developing consumer policy based on an assessment of consumer problems, which could be applied to dark commercial patterns (OECD, 2010[23]).

[3] In principle dark commercial patterns also exist offline, where for example the choice architecture in a brick-and-mortar store is configured so as to misdirect consumers into spending more than they would otherwise want. But as the concept is mainly used with regard to the digital world, in this document references to dark commercial patterns relate solely to online instances.

[4] To illustrate the length of popular apps' terms and policies, in 2016, the Norwegian Consumer Council (NCC) read out the terms of service and privacy policies of an average smartphone's apps word by word in real time, which took around 32 hours. See https://www.forbrukerradet.no/side/the-consumer-council-and-friends-read-app-terms-for-32-hours/ for further details. The CCP has also separately developed guidance on how behavioural insights can improve online disclosures (OECD, 2018[7]).

[5] A joint policy note of the CCP and Working Party on Consumer Product Safety (WPCPS) further discusses the prevalence of dark commercial patterns on online marketplaces (OECD, 2021[26]).

[6] The 2016 OECD E-commerce Recommendation also provides that "Businesses should take special care in advertising or marketing that is targeted to children, vulnerable or disadvantaged consumers, and others who may not have the capacity to fully understand the information with which they are presented" (OECD, 2016[25]).

[7] See e.g. https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html and Calo and Rosenblat (2017[22]).

[8] The EU's Directive 2005/29/EC, the Unfair Commercial Practices Directive ('UCPD'), prohibits unfair commercial practices and provides that the unfairness of a practice shall be assessed by the impact it has on the average consumer. It also provides that the unfairness of practices likely to affect only a group of consumers who are particularly vulnerable to the practice because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee, shall be assessed by the impact on the average member of that group: https://eur-lex.europa.eu/eli/dir/2005/29/oj. But in a forthcoming study conducted for the European Consumer Organisation (BEUC) on the concept of digital vulnerability in relation to the UCPD, researchers have suggested that in digital markets the vulnerable consumer is no longer the exception, nor is the average consumer the rule. Instead, every consumer could be considered to have a persuasion profile making them more or less vulnerable to certain practices and at certain times. (Helberger et al., forthcoming[21]).

[9] Such as the Netherlands Consumer & Markets Authority and the UK Competition & Markets Authority.

[10] Indeed the EU's UCPD also provides that the unfairness of a practice can also be assessed by the impact it has on the average consumer to whom it is addressed, or the average member of a group of consumers when a practice is directed to that group.

[11] Relevantly, the final report includes appendices covering consumer controls over platforms' data collection (Appendix K), a summary of research on consumer attitudes and behaviour (Appendix L), and an example of appropriate choice architecture incorporating fairness by design (Appendix Y). See https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study for details.

[12] See e.g. Morton et al. (2019[27]).

[13] Regulation (EU) 2016/679, known as the General Data Protection Regulation ('GDPR'), provides that unless the processing of a data subject's data is necessary for certain permitted reasons such as protecting the data subject's vital interests or complying with a legal obligation, the data subject must provide consent for the processing of their data. Consent of the data subject is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". For details, see https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[14] For example, the European Commission has suggested that the dark commercial pattern termed "bait-and-switch" could fall afoul of ban no.6 in the UCPD blacklist (Annex I). Similarly, the EU Consumer Rights Directive, which bans pre-selected options under Article 22, may extend to the dark commercial patterns known as "hidden charges" or "sneak into basket". (European Commission, 2019[24]). As part of the EC's New Deal for Consumers initiative to modernise EU consumer law, further practices were recently added to the UCPD blacklist, including in relation to false reviews (see https://eur-lex.europa.eu/eli/dir/2019/2161/oj for details) - such a ban may extend to the dark commercial pattern "testimonial of uncertain origin".

[15] See https://www.bmjv.de/DE/Themen/FokusThemen/CDR_Initiative/CDR_Initiative_EN_node.html for more details.

[16] See https://www.gov.uk/government/publications/summary-of-the-court-order-secured-by-the-cma-against-viagogo for details.