OECD publishing

CONSUMER VULNERABILITY IN THE DIGITAL AGE

OECD DIGITAL ECONOMY PAPERS
June 2023 **No. 355**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

Protecting consumers when they are most vulnerable has long been a core focus of consumer policy. This report first discusses the nature and scale of consumer vulnerability in the digital age, including its evolving conceptualisation, the role of emerging digital trends, and implications for consumer policy. It finds that in the digital age, vulnerability may be experienced not only by some consumers, but increasingly by most, if not all, consumers. Accordingly, it sets out several measures to address the vulnerability both of specific consumer groups and of all consumers, and concludes on avenues for more research on the topic.

The report was prepared by Nicholas McSpedden-Brown and Reiko Odoko, under the supervision of Brigitte Acoca of the OECD Secretariat. It was approved and declassified by written procedure by the Committee on Consumer Policy on 31 March 2023 and prepared for publication by the OECD Secretariat.

The report was developed with the support of a voluntary contribution from the Consumer Affairs Agency, Government of Japan.

Note to Delegations:

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

DSTI/CP(2021)7/FINAL

Corrigendum

An earlier version of this report from 26 June 2023 was revised:

Page 2, **third paragraph:** inclusion of sentence “The report was developed with the support of a voluntary contribution from the Consumer Affairs Agency, Government of Japan.”
Page 32, **third paragraph:** change of font style of quote to italics.
Page 36, Table 2, column “Regulatory measure”, row “Japan”: change of “surcharges” to “Orders for Action”.

Avant-propos

Protéger les consommateurs lorsqu'ils sont particulièrement vulnérables est depuis longtemps une priorité phare des politiques en matière de consommation. Le présent rapport examine la nature et l'ampleur de la vulnérabilité des consommateurs à l'ère du numérique, notamment l'évolution de sa conceptualisation, le rôle des nouvelles tendances propres au numérique et les incidences sur l'élaboration des politiques de consommation. Il révèle qu'à l'ère du numérique, la vulnérabilité peut concerner non plus seulement certains consommateurs, mais la plupart d'entre eux, sinon tous. En conséquence, il énonce plusieurs mesures qui permettraient de parer à la vulnérabilité de groupes particuliers et de l'ensemble des consommateurs, avant d'envisager des pistes de travaux de recherche supplémentaires sur le sujet.

Ce rapport a été élaboré par Nicholas McSpedden-Brown et Reiko Odoko, sous la supervision de Brigitte Acoca, du Secrétariat de l'OCDE. Il a été approuvé et déclassifié selon la procédure écrite par le Comité de la politique à l'égard des consommateurs, le 31 mars 2023, et préparé pour publication par le Secrétariat de l'OCDE.

Le rapport a été élaboré avec le soutien d'une contribution volontaire de l'Agence de la consommation, gouvernement du Japon.

Note aux délégations :

Ce document est également disponible sur O.N.E sous la cote :

DSTI/CP(2021)7/FINAL

Corrigendum

Une version antérieure de ce rapport datant de 26 juin 2023 a été révisée comme suit :

Page 3, troisième paragraphe : inclusion de la phrase « Le rapport a été élaboré avec le soutien d'une contribution volontaire de l'Agence de la consommation, gouvernement du Japon ».
Page 32, troisième paragraphe : modification du style de police de la citation en italique.
Page 36, Tableau 2, colonne « Regulatory measure », rangée « Japan » : changement de « surcharges » à « Orders for Action » (en anglais).

Table of contents

Executive summary

Emerging digital trends may point to a new conceptualisation of consumer vulnerability

Protecting consumers when they are most vulnerable has long been a core focus of consumer policy makers and authorities. But consumer vulnerability is a complex and multi-dimensional concept that has no globally accepted definition. Under a traditional conceptualisation, the "class-based approach", specific consumer groups are regarded as inherently vulnerable owing to certain characteristics, such as their age or education level.

Yet several trends illustrate how in the digital age, vulnerability may be experienced not only by some consumers, but increasingly by the vast majority of, if not all, consumers. Specifically, while rapid uptake of e-commerce (particularly since the COVID-19 outbreak) has empowered consumers in many ways, consumers have been increasingly exposed to problems. During the pandemic, scams, unfair practices in cancellations and refunds and price gouging abounded online, affecting many consumers. Today, many consumers struggle in online transactions, which are increasingly subscription-based or non-monetary (i.e. where consumers "pay" with their data), and require reliance on indicators of quality or safety that are harder to assess online. In addition, dark commercial patterns, business practices employing elements of digital choice architecture that subvert consumer decision-making (e.g. pressuring a purchase with a fake countdown timer), have proliferated. Moreover, practices leveraging consumer data to personalise advertising, pricing and other aspects, while presenting benefits, may increasingly be used to exploit consumers' individual vulnerabilities. Growing business use of algorithms employing artificial intelligence, e.g. to determine eligibility for services, may also increase risk of bias and discrimination against specific consumer groups. Against this backdrop, digital divides in access and use of digital technologies remain, driven by gaps in digital literacy, skills and connectivity.

While evidence of the extent of harms from many of these new digital practices is still emerging, some stakeholders have called for a new conceptualisation of consumer vulnerability as universal or systemic. Such an approach largely aligns with the 2014 OECD Recommendation on Consumer Policy Decision-making's conceptualisation, according to which all consumers may at times be vulnerable to detriment, depending on 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.

Potential implications for consumer policy and law

In the same vein, policy research and guidance have reflected a shift in recent years towards a "state-based approach" that views consumer vulnerability to result from the combination of temporary and permanent factors both internal and external to the consumer. Some jurisdictions also anchor a broader view of consumer vulnerability in the law, including through provisions stating that all consumers may be vulnerable. Jurisdictions employing the legal standard of an "average" or "reasonable" consumer to assess potentially unfair or deceptive commercial practices, such as the European Union or the United States, may do so too, to the extent that those standards may be adaptable to digital market realities and a more realistic understanding of consumers (e.g. as being prone to behavioural biases). Still, some have questioned whether the distinction between an "average" or "reasonable" consumer and a "vulnerable"

consumer continues to be relevant, especially as digital practices may increasingly affect all consumers. More evidence on the continued appropriateness of such standards is thus needed.

In any case, to the extent consumer vulnerability online is increasingly systemic, the line between addressing consumer vulnerability and protecting all consumers will increasingly be blurred – even if at times some consumer groups will continue to warrant specific attention. This implies a continuing need for measures to address the vulnerability of specific consumer groups, but also, increasingly, of consumers in general in the digital environment.

Measures to address the vulnerability of specific and all consumers

Many jurisdictions provide legal protections for specific consumer groups understood as vulnerable, including online. In particular, many regulatory measures address practices affecting children in online transactions – specifically regarding advertising, collection and use of children's personal data and in-game purchases. Consumer authorities have also engaged in targeted monitoring and enforcement, conducted education and awareness campaigns and issued guidance in relation to the protection and empowerment, including online, of certain consumer groups – particularly children, the elderly, and consumers with less digital access and literacy. This is complemented by international awareness campaigns and self-regulatory initiatives.

Existing measures in many jurisdictions also address consumer vulnerability more broadly online, in particular prohibitions on deceptive, fraudulent and unfair practices, which have served to tackle e.g. online fraud during the pandemic or dark patterns. Consumer laws may in some circumstances also address exploitative personalisation practices and discriminatory algorithms, as may privacy and data protection, competition and non-discrimination laws. But there are few enforcement actions to confirm their adequacy so far, owing in part to the novelty of such practices. Partly in response to regulatory gaps, new measures have been implemented addressing the risks highlighted above. These include updates to consumer, product safety, privacy and data protection laws, as well as cross-cutting approaches focusing on online platforms or data portability. Proposals have also been made for targeted measures addressing dark patterns, exploitative personalisation practices and algorithmic discrimination.

Strengthening the evidence base by using traditional and novel methods

More evidence on consumer vulnerability is needed. Research has to date mainly focused on certain personal attributes and circumstances, such as age and income, rather than external conditions (e.g. digital market practices), individual states (e.g. emotions) and other attributes or circumstances (e.g. geographical remoteness). Traditional empirical methods, such as surveys, behavioural experiments, complaints analysis, focus groups and interviews, are promising avenues for capturing data on several of such less-researched factors. Though studying the temporal or contextual vulnerabilities peculiar to the digital environment may require novel methods, e.g. involving studying "digital trace" data or the outputs of businesses' algorithms.

The OECD Committee on Consumer Policy will continue to develop evidence on consumer vulnerability in its research agenda, working with other international fora and stakeholders. This includes, in particular, empirical work aimed to assess consumer attitudes and behaviour towards dark patterns, sustainable consumption and online product safety, to be undertaken over the course of 2023-2024.

Résumé

Les tendances qui se font jour à l'ère du numérique pourraient ouvrir la voie à une nouvelle conceptualisation de la vulnérabilité des consommateurs

Protéger les consommateurs lorsqu'ils sont particulièrement vulnérables est depuis longtemps une priorité phare des responsables des politiques de consommation et des autorités compétentes. Toutefois, la vulnérabilité des consommateurs est une notion complexe et pluridimensionnelle dont il n'existe pas de définition universellement admise. Selon une approche traditionnelle « fondée sur des classes », des groupes de consommateurs particuliers sont considérés comme intrinsèquement vulnérables du fait de certaines caractéristiques, telles que l'âge ou le niveau d'instruction.

Or plusieurs évolutions montrent qu'à l'ère du numérique, la grande majorité des consommateurs, sinon tous, peuvent se retrouver en situation de vulnérabilité. De fait, si l'adoption rapide du commerce électronique (en particulier depuis le début de la pandémie de COVID-19) a ouvert le champ des possibles pour les consommateurs, elle les expose de plus en plus à des problèmes. Pendant la pandémie, les escroqueries, pratiques déloyales dans le cadre des annulations et remboursements, et prix abusifs se sont multipliés, affectant de nombreux internautes. Aujourd'hui, il n'est pas rare que les consommateurs rencontrent des problèmes lors de leurs transactions en ligne, qui sont de plus en plus fréquemment basées sur des abonnements ou non monétaires (leurs données servant alors de monnaie d'échange) et obligent à se fier à des indicateurs de qualité ou de sécurité plus difficiles à évaluer dans l'environnement numérique. À cela s'ajoute la prolifération des interfaces commerciales truquées, ces pratiques d'entreprises faisant intervenir des éléments d'architecture de choix numérique qui influencent la prise de décision des consommateurs (en recourant par exemple à un faux compte à rebours pour les pousser à procéder à un achat). De plus, les pratiques consistant à mettre à profit les données des consommateurs pour personnaliser la publicité, la tarification et d'autres aspects présentent certes des avantages, mais tendent également à être utilisées pour exploiter les vulnérabilités particulières des consommateurs. Le recours croissant aux algorithmes fondés sur l'intelligence artificielle, pour déterminer par exemple l'accès à des services, peut en outre renforcer le risque de biais et de discrimination contre des groupes spécifiques de consommateurs. Dans ce contexte, les fractures numériques en matière d'accessibilité et d'utilisation des cybertechnologies demeurent, du fait des écarts de maîtrise du numérique, de compétences et de connectivité.

Si l'on dispose encore de peu de données attestant de l'étendue des préjudices causés par ces nouvelles pratiques numériques, certaines parties prenantes ont appelé à une nouvelle qualification de la vulnérabilité des consommateurs comme universelle ou systémique. Une telle approche va globalement dans le sens de la conceptualisation proposée dans la Recommandation de l'OCDE de 2014 sur le processus d'élaboration des politiques publiques en matière de consommation, selon laquelle tous les consommateurs peuvent être vulnérables à un préjudice à un moment particulier, du fait des caractéristiques du marché d'un produit donné, des propriétés du produit, de la nature de la transaction ou de l'état ou de la situation du consommateur.

Incidences potentielles sur la politique et la législation en matière de consommation

Dans la même veine, les travaux de recherche et les orientations pratiques reflètent un virage, amorcé depuis quelques années, vers une approche « étatique » qui aborde la vulnérabilité des consommateurs comme le résultat d'une conjonction de facteurs temporaires et permanents, à la fois propres et extérieurs aux consommateurs. Certains pays et territoires inscrivent également dans la loi une vision plus large de la vulnérabilité, en introduisant notamment des dispositions stipulant que tous les consommateurs pourraient être vulnérables. Ceux qui prennent comme norme juridique un consommateur « moyen » ou « raisonnable » pour évaluer d'éventuelles pratiques commerciales déloyales ou trompeuses, comme l'Union européenne ou les États-Unis, pourraient en faire de même, dans la mesure où ces normes pourraient être adaptées à la réalité des marchés numériques et à une compréhension plus réaliste des consommateurs (comme étant sujets à des biais comportementaux, par exemple). Pour autant, certains se demandent si la distinction entre un consommateur « moyen » ou « raisonnable » et un consommateur « vulnérable » reste pertinente, d'autant que les pratiques numériques pourraient toucher tous les consommateurs. Il importe par conséquent d'étoffer la base factuelle sur la persistance du bien-fondé de ces normes.

Quoi qu'il en soit, dans la mesure où la vulnérabilité des cyberconsommateurs tend à devenir systémique, la frontière entre la gestion des vulnérabilités et la protection de l'ensemble des consommateurs sera de plus en plus floue – même si des groupes spécifiques continueront dans certains cas de nécessiter une attention particulière. Cela implique de continuer de prévoir des mesures pour parer aux vulnérabilités non seulement de groupes de consommateurs précis, mais aussi de l'ensemble des consommateurs évoluant dans l'environnement numérique.

Mesures visant à parer aux vulnérabilités de consommateurs particuliers et de l'ensemble des consommateurs

De nombreux pays et territoires prévoient des protections juridiques pour des groupes de consommateurs spécifiques considérés comme vulnérables, y compris dans l'environnement numérique. Nombre de mesures réglementaires visent en particulier les pratiques liées à la participation des enfants aux transactions en ligne – publicité, collecte et utilisation des données à caractère personnel des enfants, ou achats intrajeux. Les autorités chargées de la protection des consommateurs ont également mis en place des activités ciblées de surveillance et de contrôle de l'application des lois, mené à bien des campagnes d'information et de sensibilisation et formulé des orientations sur la protection et l'autonomisation, notamment en ligne, de certains groupes de consommateurs – en particulier les enfants, les personnes âgées et les individus bénéficiant d'un accès au numérique plus limité et d'une moindre maîtrise technologique. À cela s'ajoutent les programmes de sensibilisation internationaux et les initiatives d'autoréglementation.

De nombreux pays et territoires ont également pris des mesures ayant trait plus largement à la vulnérabilité des consommateurs en ligne et interdisant notamment les pratiques commerciales trompeuses, frauduleuses et déloyales, qui ont aidé par exemple à lutter contre la fraude en ligne pendant la pandémie ou contre les interfaces truquées. Par ailleurs, les lois relatives à la protection des consommateurs peuvent dans certains cas viser les pratiques de personnalisation à des fins d'exploitation et l'utilisation d'algorithmes à l'origine de discriminations ; il en va de même des lois en matière de protection de la vie privée et des données, de concurrence et de lutte contre la discrimination. Toutefois, peu d'activités de contrôle attestent de leur pertinence jusqu'à présent, notamment parce que ces pratiques sont récentes. Face entre autres aux lacunes des réglementations, de nouvelles mesures ont été mises en œuvre pour réduire les risques précités. L'objectif est d'actualiser les lois en matière de consommation, de sécurité des produits et de protection de la vie privée et des données, ou d'adopter des approches transversales axées sur les plateformes électroniques ou la portabilité des données. Des mesures ciblées sont

également proposées pour lutter contre les interfaces commerciales truquées, les pratiques de personnalisation à des fins d'exploitation et la discrimination algorithmique.

Enrichir la base factuelle en utilisant des méthodes traditionnelles et nouvelles

Il convient d'étoffer la base factuelle sur la vulnérabilité des consommateurs. Jusqu'à présent, les travaux de recherche ont été essentiellement centrés sur des attributs et des circonstances personnels, tels que l'âge et les revenus, plutôt que sur des conditions exogènes (comme les pratiques sur les marchés numériques), des états individuels (des émotions, par exemple) et d'autres attributs ou conditions (tels que l'éloignement géographique). Les méthodes empiriques traditionnelles, à l'image des enquêtes, des expériences comportementales, de l'analyse des réclamations, et des groupes de réflexion et entretiens, pourraient aider à recueillir des données sur plusieurs de ces facteurs moins étudiés. Toutefois, l'examen des vulnérabilités temporelles ou contextuelles propres à l'environnement numérique pourrait exiger de recourir à des méthodes novatrices, telles que l'analyse des « traces numériques » ou des résultats des algorithmes des entreprises, par exemple.

Le Comité de la politique à l'égard des consommateurs de l'OCDE continuera d'enrichir la base factuelle sur la vulnérabilité des consommateurs dans le cadre de ses travaux de recherche, en collaboration avec d'autres forums internationaux et les parties prenantes concernées. À ce titre, on mènera, en 2023-24, des travaux empiriques afin d'évaluer l'attitude et le comportement des consommateurs à l'égard des interfaces commerciales truquées, de la consommation durable et de la sécurité des produits vendus en ligne.

Introduction

Addressing consumer vulnerability has been central to the OECD Committee on Consumer Policy's (CCP) work since its inception, and the need for consumer policy makers to give special attention to vulnerable consumers was specifically highlighted in the 1999 Guidelines for Consumer Protection in the Context of Electronic Commerce[1] and the 2010 OECD Consumer Policy Toolkit (OECD, 2010[1]).

Principles on protecting vulnerable consumers have also featured in:

- the 2007 OECD Recommendation on Consumer Dispute Resolution and Redress [OECD/LEGAL/0356]
- the 2014 OECD Recommendation on Consumer Policy Decision Making [OECD/LEGAL/0403]
- the 2016 OECD Recommendation on Consumer Protection in E-commerce [OECD/LEGAL/0422] (which revised the 1999 Guidelines)
- the 2020 OECD Recommendation on Consumer Product Safety [OECD/LEGAL/0459]
- the 2021 OECD Recommendation on Children in the Digital Environment [OECD/LEGAL/0389].

Today's rapidly changing and increasingly complex global digital environment has delivered many benefits, but also given rise to new forms of consumer detriment. In 2019, as part of an international consumer conference organised under the G20 Presidency of Japan, the CCP highlighted the challenges to understanding and addressing consumer vulnerability in the digital age, noting there are circumstances where all consumers may be vulnerable (OECD, 2019[2]). As part of its 100th Session in April 2021, the CCP held a roundtable that explored ongoing and emerging consumer issues associated with the changing nature and extent of consumer vulnerability in the digital age. The roundtable examined how consumer vulnerability is evolving in the digital era as a result of various factors, including different and changing consumer behaviour in the online world; the risk of algorithmic discrimination; increased data collection, consumer profiling and personalisation; and potentially harmful digital choice architectures (known as "dark commercial patterns"). Participants also suggested a need to develop more evidence on the detriment suffered by vulnerable consumers, to facilitate more effective policy and enforcement responses to address consumer vulnerability (Annex A provides a summary of the discussion).

Following the event, the CCP agreed to develop this report to further explore the evolution of consumer vulnerability in the digital age and identify possible responses. This report is divided into three main sections discussing:

- the nature of consumer vulnerability in the digital age, including its evolving conceptualisation, the role of emerging digital trends, and implications for consumer policy and law (Section 1)
- possible measures to address consumer vulnerability online (Section 2)
- possible ways to strengthen the evidence base regarding consumer vulnerability online (Section 3).

The report was developed consistently with related CCP projects on dark commercial patterns (OECD, 2022[3]) and measuring financial consumer detriment in e-commerce (OECD, 2022[4]), as well as a joint workshop with the OECD Competition Committee held in April 2023 on behavioural insights in consumer and competition policy, which covered dark patterns and exploitative personalisation practices.[2] The CCP

and its Working Party on Consumer Product Safety (WPCPS) are also currently developing several projects building on the findings of this report, including:

- empirical work on dark commercial patterns and how they affect consumer vulnerability
- a new focus on use of AI to detect and mitigate consumer risks online
- methodological work on approaches to measuring i) the impacts of consumer policy interventions, including in mitigating consumer vulnerability; and ii) the costs of unsafe products.

1 What is consumer vulnerability in the digital age?

The evolving conceptualisation of consumer vulnerability

Conceptualisation in academic literature

Protecting consumers when they are most vulnerable has long been a core focus of consumer policy makers and authorities. Consumer vulnerability is a complex, multi-dimensional concept. At its most basic level, it means susceptibility to harm (Smith and Cooper-Martin, 1997[5]). Yet it has no universally accepted definition and the academic literature on the topic is fragmented (Rotzmeier-Keuper, 2020[6]; Kaprou, 2020[7]; Hill and Sharma, 2020[8]). Researchers have identified two broad kinds of conceptualisation in the literature (Kaprou, 2020[7]; Rotzmeier-Keuper, 2020[6]):

- One, termed the "class-based approach", considers consumer vulnerability in terms of specific groups of consumers that are inherently or persistently vulnerable as a result of individual characteristics, such as their age or education level (see e.g. Commuri and Ekici (2008[9]) and Shultz and Holbrook (2009[10])).
- A second, termed the "state-based approach" and put forward more recently in the literature, considers consumer vulnerability to result from the combination and interaction of factors both internal and external to the consumer, which may be temporary or permanent in duration (Baker, Gentry and Rittenburg, 2005[11]; Hill and Sharma, 2020[8]; Albertson Fineman, 2008[12]; Helberger et al., 2021[13]).

The class-based approach has been criticised in several respects, including for stigmatising particular groups of consumers (Cole, 2016[14]; Brown, 2011[15]); for lack of nuance in characterising entire groups of consumers as inherently vulnerable (Hill and Sharma, 2020[8]); for missing the root causes of vulnerability (e.g. cognitive impairment or limited impulse control) (Duivenvoorde, 2015[16]); and for ignoring other factors that may contribute to vulnerability such as those relating to the market (Commuri and Ekici, 2008[9]). In contrast, the state-based approach has been argued to have the advantage of allowing a range of factors to drive vulnerability and for all consumers to potentially be vulnerable, depending on individual and environmental circumstances. Proponents of the state-based approach submit that external factors, particularly commercial practices that exploit vulnerabilities, may be equally or more determinative of consumer vulnerability than internal factors (Helberger et al., 2021[13]). Indeed, some empirical evidence shows that some socio-demographic characteristics do not necessarily drive consumer vulnerability as much as traditionally thought (see Box 1 below regarding elderly consumers). Implicit in this approach is the notion that vulnerability has multiple perspectives; for instance, Duivenvoorde (2015[16]) highlights vulnerability may be viewed not only from the point of view of the *limited abilities* of some consumers to deal with commercial practices, but also in terms of the *degree of exposure* to certain commercial practices and the *consequences* of those practices. In a similar vein, Cartwright (2014[17]) distinguishes informational, pressure, supply, redress and impact vulnerability.

Nonetheless, it has been argued that the class-based approach has the advantage of providing clarity and legal certainty in a policy context as to who is considered vulnerable (Baker and Mason, 2011[18]; Kaprou,

2020[7]) and may assist with proactive policy development (Commuri and Ekici, 2008[9]; Rotzmeier-Keuper, 2020[6]). In contrast, the state-based approach has been criticised for the difficulty in acknowledging distinctions between particularly vulnerable consumers (Cole, 2016[14]). Though some proponents of the state-based approach also refer to the concept of "disadvantaged" consumers, understood as worse off than other consumers in a given context (Hill and Sharma, 2020[8]), which may or may not make them more susceptible to harm in that context.[3] Helberger et al. (2021[13]) further clarify that even if consumers may all be vulnerable to manipulation under the state-based approach, as both cognitive and technical resources and cognitive limitations and biases are not distributed evenly among the population, some consumers will inevitably be at greater risk than others.

Conceptualisation in national and international policy documents

OECD consumer policy reports and Recommendations have conceptualised consumer vulnerability in different ways. Specifically, the 2007 OECD Recommendation on Consumer Dispute Resolution and Redress broadly relies on a class-based approach, noting that: *"Disadvantaged or vulnerable consumers refers to particular consumers or categories of consumers, who because of personal characteristics or circumstances (e.g. age, mental or physical capacity, education, income, language or remote location) may meet particular difficulties in accessing dispute resolution and redress"* (OECD, 2007[19]).

In contrast, the 2010 OECD Consumer Policy Toolkit ("the Toolkit") notes: *"All consumers can be vulnerable to detriment. They are, however, likely to be more susceptible at some times than others. Vulnerability may be due to a consumer's psychological or financial state or the nature of a transaction. Service providers might, for example, be in good position to prey upon a grieving person's sense of remorse and guilt to sell a higher-priced or overpriced product that the consumer would normally pass up. Moreover, research indicates that consumers may also be vulnerable by reasons of the place or context in which purchases take place"* (OECD, 2010[1]).

Similar to some scholars, the Toolkit distinguishes *vulnerable* from *disadvantaged* consumers, with the latter characterised as consumers who may be susceptible to detriment on a persistent basis. Examples of disadvantaged consumer groups listed in the Toolkit are those with the following characteristics: targets of discrimination (e.g. racial, ethnic or gender); low levels of (formal) education or literacy levels; language limitations (e.g. non-native speaker); immigrants and other outsiders who do not have local knowledge; impaired vision, hearing, or mobility; learning difficulties or cognitive impairment, such as dementia; restricted mobility; restricted means of communication; geographical remoteness; unemployment; or low income (OECD, 2010[1]). Such a distinction between disadvantaged and vulnerable consumers may be seen as mirroring the distinction between the class- and state-based approach to conceptualising vulnerability, with disadvantaged consumers viewed as vulnerable because of relatively persistent personal attributes and circumstances. The UN Guidelines on Consumer Protection similarly take up the distinction between vulnerable and disadvantaged consumers, though do not provide a definition of the concepts (UNCTAD, 2015[20]).

The 2014 OECD Recommendation on Consumer Policy Decision Making ("the 2014 Recommendation"), which codified parts of the Toolkit, broadly reflects a state-based approach in recognising that all consumers, regardless of education or experience, may at times be vulnerable to detriment (OECD, 2014[21]). It defines vulnerable consumers as follows: *"Vulnerable consumers are 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."* The Recommendation also defines disadvantaged consumers in the same way as the Toolkit.

Subsequent consumer policy-related OECD Recommendations, while not providing a definition of vulnerable consumers, have differed in their approach to characterising certain groups as vulnerable or disadvantaged. Specifically, the 2016 OECD Recommendation on Consumer Protection in E-commerce

does not explicitly classify specific consumer groups as vulnerable or disadvantaged consumers, though it singles out children, noting "*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*" (provision 18) (OECD, 2016[22]).[4] The 2021 OECD Recommendation on Children in the Digital Environment, while not explicitly categorising children as inherently vulnerable, recognises in its preface that children engaging online may be exposed to a spectrum of risks (including consumer risks), to which they might be more vulnerable than adults (OECD, 2021[23]). In contrast, the 2020 OECD Recommendation on Consumer Product Safety explicitly considers children, the elderly and disabled people to be either vulnerable or disadvantaged consumers: "*vulnerable and disadvantaged consumers, such as children, the elderly and disabled people*" (provision 5) (OECD, 2020[24]).

In recent years, policy research in several jurisdictions has reflected a shift towards the state-based approach to conceptualising consumer vulnerability (Kaprou, 2020[7]). In particular, a 2016 European Commission (EC) study ("the 2016 EC vulnerability study") (EC, 2016[25]) recognised that vulnerability is a dynamic concept, such that no specific group of consumers is always vulnerable or always not vulnerable (Kaprou, 2020[7]; Helberger et al., 2021[13]; Riefa, 2020[26]). The study outlined several key drivers of vulnerability: behavioural drivers, market-related drivers/problematic practices, access drivers, situational drivers and personal and demographic characteristics. It defined a vulnerable consumer as *"A consumer, who, as a result of socio-demographic characteristics, behavioural characteristics, personal situation, or market environment: 1) Is at higher risk of experiencing negative outcomes in the market; 2) Has limited ability to maximise their well-being; 3) Has difficulty in obtaining or assimilating information; 4) Is less able to buy, choose or access suitable products; or 5) Is more susceptible to certain marketing practices"* (EC, 2016[25]).

Recent policy research and guidance in other jurisdictions also reflect an approach that goes beyond internal factors. For example, the UK Competition and Markets Authority (CMA) makes the distinction between two broad categories of consumer vulnerability (CMA, 2019[27]): "market-specific vulnerability", deriving from the specific context of particular markets, and affecting a broad range of consumers within those markets; and "vulnerability associated with personal characteristics", such as physical disability, poor mental health or low incomes, which the CMA notes may result in individuals with those characteristics facing particularly severe, persistent problems across markets. The Australian Competition and Consumer Commission (ACCC) adopted a similar approach in considering that business practices and complex products exacerbate vulnerability (ACCC, 2021[28]), and sector-specific regulators in both countries have similarly adopted broad conceptualisations of consumer vulnerability (FCA, 2015[29]; Ofgem, 2013[30]; ASIC, 2019[31]). Likewise, the Consumer Education Guidelines of Portugal adopt a broad understanding in defining "vulnerable consumer" as *"Any citizen whose autonomy of choice is compromised vis-à-vis the professional or business. This lack of autonomy may be due to: endogenous factors observable in a heterogeneous group composed of people permanently considered as such because of their mental, physical or psychological condition, age or credulity (e.g. children or elderly people); exogenous factors such as education, social and financial situation, digital literacy, asymmetric information, which place these consumers in a situation of temporary or permanent weakness"* (Dias et al., 2019[32]). Similarly, guidance from the Chilean consumer protection authority (SERNAC) describes all consumers as structurally vulnerable vis-à-vis suppliers of goods and services, noting that this condition can be exacerbated by market circumstances and failures as well as characteristics of consumers (SERNAC, 2021[33]).

Emerging digital trends affecting the nature and extent of consumer vulnerability

Helberger et al. (2021[13]) contend that consumers are not inherently vulnerable, but rather that the interaction between market phenomena and consumers' differing internal attributes and circumstances causes, and can exacerbate, consumer vulnerability, including by causing disproportionate detriment to

some consumers. This sub-section explores, through this lens, how developments in the digital age may be affecting the nature and extent of consumer vulnerability. These include a rapid uptake of e-commerce, accelerated by the pandemic, and related risks; the increasing complexity of online transactions and technologies; the proliferation of dark commercial patterns; the growing potential for exploitative personalisation practices; increasing risks of biased and discriminatory algorithms; and the continuing digital divides in many countries.

Rapid uptake of e-commerce, accelerated by the pandemic, and related risks

E-commerce has grown rapidly in recent years, with the percentage of consumers who purchased online in OECD countries standing at 67% in 2022, up from 36% in 2010.[5] The COVID-19 crisis has further pushed consumers to engage in digital markets, including many first-time users: in several countries and regions, such as the European Union, the United States and Korea, e-commerce retail grew significantly faster than retail overall during the pandemic (OECD, 2021[34]).

E-commerce has in many ways empowered consumers, including through easy access to an array of competitively priced goods and services from a range of online businesses both domestically and abroad. There is also an abundance of information concerning the choices available, which can translate to greater transparency on price, quality and the reputations of providers. This has contributed to eroding traditional information asymmetries between consumers and businesses (OECD, 2018[35]). E-commerce has also provided access to markets to certain subsets of consumers, such as many disabled consumers, from which they may previously have been excluded (Simpson, 2020[36]).

But it has also exposed many consumers to problems. According to a CCP consumer survey conducted in 2021 measuring consumer detriment in e-commerce in 13 countries ("the 2021 CCP survey"), 50% of online consumers faced at least one problem in e-commerce in the year preceding the survey rollout (OECD, 2022[4]). The resulting financial detriment was found to be significant, reaching (after accounting for any redress received) up to 3.1% of the total e-commerce market size in some countries. Certain subsets of consumers were also more likely to have encountered problems – specifically younger and male consumers, consumers of higher education, in economic distress, and in rural areas. Excepting consumers with high education, these groups also faced a significantly higher magnitude of detriment (relative to the value of the products they purchased) and a lower likelihood of obtaining redress sufficient to cover the initial financial loss suffered from a problem (OECD, 2022[4]).

Problems with e-commerce were further exacerbated by the COVID-19 crisis. For example, many online consumers were exploited by unfair, misleading and fraudulent practices during the COVID-19 crisis (OECD, 2020[37]). Indeed, the 2021 CCP survey found around 25% of the most serious problems faced by consumers were related to the COVID-19 crisis. The nature of such problems varied; fraud, including scams, as well as cancellation issues were common, with the 2021 CCP survey indicating that consumers facing problems related to scams or terms and conditions were particularly likely to associate the problem faced with COVID-19 (OECD, 2022[4]). Complaint data in the United States and Australia indicate that online scams, e.g. related to fake coronavirus treatment or prevention, saw a substantial rise during the pandemic, and even experienced consumers encountered difficulties (US FTC, 2020[38]; ACCC, n.d.[39]). Because of the profound effect that the COVID-19 crisis had on older consumers, scams promoting fake cures disproportionately impacted them (US FTC, 2021[40]). From 10 March to 19 April 2020, the CMA received almost 21 000 complaints about coronavirus-related issues, particularly unfair practices in cancellations and refunds – 74% of which related to goods and services bought online (CMA, 2020[41]). In Japan, due to delays in the roll-out of vaccination, scammers professed to offer preferential access to vaccines in exchange for money (CAA, 2021[42]). Price gouging on e-commerce websites was also prevalent, with many businesses or individuals seeking to maximise profits from increased demand for essential goods such as facemasks and hand sanitiser, or basic grocery items or printers, by exponentially raising their prices (OECD, 2020[37]). The crisis also heightened risks associated with the safety of products

sold online for all consumers, illustrated by the large number of recall notices for faulty or sub-standard facemasks (OECD, 2020[37]).

Overall, the scale of consumer problems online brought about by the pandemic has illustrated how consumers across a range of different subsets, whether low- or high-income or education, young or old, could be vulnerable in e-commerce, and how the vulnerabilities of certain consumers could be exacerbated (Riefa, 2020[43]; OECD, 2020[37]). This is in part due to the increasing complexity of online transactions, as discussed below.

Increasing complexity of online transactions and technologies

The online and digital environment is increasingly defined by complex transactions and new technologies and business practices, exposing all consumers to greater risk of detriment - both financial and non-financial - and some disproportionately so.

First, there is substantial evidence that consumers tend to behave differently online than offline. Online, consumers have been found to pay less attention, process information less well, default to simplified rules of thumb when faced with information overload (Firth et al., 2019[44]; Jerath, Ma and Park, 2014[45]; Mangen, Walgermo and Brønnick, 2013[46]), routinely ignore certain kinds of content (Willis, 2020[47]) and underestimate manipulation and deception more than in offline contexts (Moran, 2020[48]).

In contrast to the offline environment, consumers are also forced to rely on other indicators to assess product quality, including search rankings, reviews, ratings and endorsements (e.g. from social influencers) – particularly on online goods and services marketplaces, which make up an increasing share of online transactions (OECD, 2022[49]). The CMA estimated that GBP 23 billion a year of UK consumer spending was influenced by online reviews (UK DBT & DSIT, 2023[50]). Such indicators have many benefits, but also create risks. In particular, many consumers face difficulties in distinguishing independent editorial content from native advertising (OECD, 2019[51]; OECD, 2019[52]), with one study finding that over 85% of study respondents could not distinguish paid-for-search ads from organic search results (KFTC, 2018[53]). Consumers with less advertising literacy or ability to understand disclosures, such as children, have particular difficulty in distinguishing advertising or endorsements, especially in social media platforms and influencer marketing (see e.g. Enke et al. (2021[54])), online games and mobile apps ("advergames") (EC, 2016[55]; OECD, 2021[56]; OECD, 2020[57]; OECD, 2019[52]). Some businesses have also been found to post fake ratings and reviews on a large scale, incentivise reviews or suppress negative reviews (OECD, 2019[58]). One survey found 52% of Australian consumers believed they had fallen victim to fake reviews.[6]

Indeed, digital innovations often make it easier to deceive consumers online with fake reviews and scams (CMA, 2019[27]). Highly genuine-looking fake reviews and testimonials can be developed through AI-based generators, [7] and fake advertising may be crafted to evade online platforms' moderation.[8] Online shopping scammers often use the latest technology to set up genuine-looking fake retailer websites, with sophisticated designs and layouts and possibly stolen logos, domain names or business identification numbers (ACCC, n.d[59]). In the United States, online shopping fraud was the most commonly reported type of fraud in which people of all ages lost money in 2020 (US FTC, 2021[40]). Online scams affect all consumers, though some scams disproportionately target those of a certain demographic, such as elderly or disabled consumers or those with language limitations (ACCC, 2021[60]). Indeed, across several countries, scams and fraud have disproportionately impacted older consumers, suggesting that they may be more vulnerable to them (see Box 1 below). For example, in 2020, US consumers aged 60 and over were two to nearly five times more likely than younger age groups to report losses from an impersonation scam, prize, sweepstakes or lottery scam, or a tech support scam (though they were still least likely of any age group to report monetary loss) (US FTC, 2021[40]). In Australia, a survey of consumers over 50 found one in four respondents reported having had their details stolen, had a virus attack or been victims of a scam (Office of the eSafety Commissioner, 2018[61]). This may relate to a higher propensity to be targeted, but also other factors such as less experience or confidence online. For example, UK consumers aged 65

years and older were found to be the least likely to check if an Internet site was secure before sharing credit card details (CMA, 2019[27]).

Box 1. Are older consumers always vulnerable?

Older consumers have traditionally been considered a vulnerable consumer group. This has often been attributed to diminished decision-making skills due to cognitive impairment that many older adults experience. Indeed research shows elderly consumers struggle more to process large amounts of information at a high pace, are less able to remain attentive and alert over long periods, and are less able to discriminate between relevant and irrelevant information (Duivenvoorde, 2015[16]). And some findings suggest that the elderly are comparatively more prone to detriment than younger consumers in certain situations, e.g. when faced with scams and fraud (see above).

But evidence also shows that elderly consumers are less prone to consumer detriment and vulnerability than younger age groups in other contexts. For example, the 2021 CCP survey showed that older consumers were less likely than younger consumers to encounter problems in e-commerce overall. With regard to the most serious problem faced in the 12 months preceding the survey, the data also suggest that older consumers, on average, faced lower financial detriment (relative to the value of the product they purchased) than younger consumers and that they were also more likely to obtain redress sufficient to cover the original financial loss suffered (OECD, 2022[4]). Similarly, a 2017 EC survey measuring consumer detriment found both the rate of problems and the magnitude of associated financial loss to be higher in younger age groups in all of the six markets covered by the study (EC, 2017[62]). A 2018 EC survey found older consumers were less likely to feel vulnerable than younger consumers, and that "felt vulnerability" was instead most closely linked to financial situation (EC, 2018[63]). Surveys in the United Kingdom, the United States and Canada found older consumers fell prey to unfair commercial practices less often than other age groups, while a survey in the Netherlands showed no correlation with age (Duivenvoorde, 2015[16]). Berg (2015[64]) found that older consumers in Norway were less likely than other age groups to make economically unfortunate consumer decisions, and considered that poor economic awareness and lack of time were instead the main vulnerability drivers. Garrett and Toumanoff (2010[65]) found that neither age, education or race correlated with the propensity for consumers to express a complaint. In fact, following a review of the literature, Duivenvoorde (2015[16]) considered that the only socio-demographic characteristics that somewhat convincingly showed a relationship to vulnerability in the literature were income, education and social class.

Why do older consumers appear more vulnerable in some contexts than others? Duivenvoorde (2015[16]) lists three reasons. First, characteristics that are commonly linked to vulnerability (such as age, income and social class) often do not directly address the cause of vulnerability: being old does not necessarily mean being inept at reaching good decisions, but it may be associated with factors that do, including other characteristics such as health conditions, sensory impairment, disability and cognitive impairment, digital exclusion, limited digital capabilities, but also potentially specific circumstances such as isolation, loneliness or bereavement (CMA, 2019[27]). Second, within a given demographic, consumers have different abilities, knowledge, experiences and personalities, such that they will not all exhibit the same behaviour. "Elderly consumers" may refer both to consumers just over 65 as well those above 90. And a sizeable senior population is as capable, or more capable in many regards, than younger persons, in large part thanks to their years of experience as consumers (OECD, 2010[1]). Finally, members of a specific consumer group are not usually vulnerable to all practices, as vulnerability is often highly context-specific; for example, consumers with physical infirmity may be more vulnerable to predatory mortgages. A final consideration relates to how data are presented: for example, while older US adults who reported losing money to scams in 2020 reported much higher median individual dollar losses than younger consumers, younger consumers were more likely to report losing money to fraud than older adults overall (US FTC, 2021[40]).

These findings confirm the 2010 OECD Consumer Policy Toolkit's guidance to exercise caution in qualifying not only elderly consumers as a vulnerable consumer group, but any particular consumer group as vulnerable. A more nuanced approach is to consider that some consumer groups can be disproportionately affected by certain practices or market phenomena at certain times, depending on a range of associated and interrelated factors.

Difficulties in assessing products online also apply to their safety, which is a key concern for all consumers. Indeed, data indicate that consumer product injuries affect consumers of all age groups, even if older adults have higher rates of injury for certain products[9] and thus may incur higher costs.[10] Data from a 2021 OECD online product safety sweep across 21 countries suggest that the average rates of non-compliance of consumer products in seven key categories (toys/games, household electrical, household non-electrical, sporting/recreation, apparel, children/infant, portable technology) with bans/products recalls, labelling requirements and safety standards are high, as an earlier OECD online product safety sweep in 2015 also showed (OECD, forthcoming[66]; OECD, 2016[67]). In addition, for many products sweep researchers were unable to determine whether a product was compliant with relevant product safety standard by online inspection alone.

New technologies, including AI, the Internet of Things (IoT) and augmented and virtual reality, are rendering e-commerce and consumer devices increasingly complex. In some respects, consumers may be empowered and rendered less vulnerable by such developments – e.g. digital assistants that make suggestions free from biases that may otherwise influence consumers (OECD, 2019[68]). However, new technologies and their use in transactions can also put many consumers at greater risk. For example, IoT and AI give rise to specific product safety, privacy, and digital security risks (OECD, 2020[69]; OECD, 2019[2]). Mobile and in-app payments may involve limited authentication controls, fostering risk of fraud (OECD, 2014[70]), while purchases made through voice-controlled digital assistants may be accompanied by more limited information disclosures (OECD, 2018[71]; OECD, 2019[52]). Facial recognition for payments also presents significant concerns related to privacy and discrimination (EPRS, 2021[72]).

Increasingly, e-commerce transactions are based on a subscription model. The subscription-based economy is reported to have grown more than 435% over 2012-2020 (Subscribed Institute, 2021[73]), with 78% of adults in a survey covering 10 OECD countries as well as the People's Republic of China and Singapore found to have a subscription service in 2020 (up from 71% in 2018) (Subscribed Institute, 2021[74]). But in selected markets based on subscriptions or auto-renewal contracts, such as telecommunications and various financial services, longstanding customers can end up paying much more than others. The CMA has characterised this as "a loyalty penalty", amounting to GBP 4 billion per year in the United Kingdom (CMA, 2019[27]). Such consumers have been conceptualised as disengaged – a type of vulnerability that may affect all consumers, whereby the prevailing market structure and commercial practices, such as obfuscation and information proliferation, lead to lack of interest to shop around or switch (EC, 2016[25]; Siciliani, Riefa and Gamper, 2019[75]). Indeed, the CMA found 70% of consumers were on highly expensive default energy tariffs, but also that, in some markets, affected consumers were disproportionately on low incomes, aged 65 or over, of lower education, unemployed or with a health condition (CMA, 2019[27]). In the same vein, UK consumers were estimated to spend GBP 1.6 billion a year on subscriptions they did not want (UK DBT & DSIT, 2023[50]). The 2021 CCP survey also showed that consumers encountering a problem with a subscription typically faced a larger number of different associated problem types (e.g. problems with delivery, understanding terms and conditions, or payment) than consumers encountering problems with a one-off purchase. Problems with subscriptions were also associated with higher detriment on average (relative to the product value) and the redress consumers obtained less frequently sufficed to fully offset any financial loss suffered (OECD, 2022[4]).

In addition, non-monetary transactions, including transactions offered for "free" or at lower prices in exchange for consumer data or attention time are an increasing part of the online environment (OECD, 2016[22]). The understanding and agency of most consumers in such transactions is limited. This results from a range of factors, including complex take-it-or-leave-it terms of service and privacy policies (that often employ "click-wrap" agreements), lack of user-friendly privacy controls, lack of awareness of the ultimate use of consumers' personal data, and digital platform market power (Forbrukerrådet, 2020[76]; Fletcher et al., 2021[77]; OECD, 2018[78]). There are also numerous challenges to ensuring effective information disclosures for such transactions, including possible information overload, consumer heterogeneity (e.g. less and more educated or literate consumers), and possible business incentives to

circumvent mandatory disclosures requirements (OECD, 2022[79]). Non-monetary transactions with online platforms are furthermore often characterised by significant bargaining power imbalances and information asymmetries (ACCC, 2019[80]; OECD, 2018[78]). The extent to which consumers can meaningfully give informed consent in such transactions is thus questionable. Many online consumers may thus be at risk in such transactions, particularly in terms of non-financial detriment, such as data breach, identity theft or misuse of personal data and other privacy harms (OECD, 2020[81]). A further difficulty is that in some jurisdictions, consumer law may not apply to non-monetary transactions (OECD, 2020[81]).

Finally, online gaming is increasingly based on a free-to-play model, where revenue is generated through the sale of in-game virtual items acquired through micro-transactions rather than of game products (Leahy, 2022[82]). Many micro-transactions occur through loot boxes, 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[83]). One study found around 60% of the top games on the Google Play and Apple stores contained loot boxes (Zendle et al, 2020[84]). Consumers prone to addiction may be particularly at risk of financial loss in such transactions, which for some commentators constitute a form of gambling. This applies to all age groups, considering that in many countries video games are played by large proportions of the population (e.g. around half of EU consumers and three quarters of US consumers (Forbrukerrådet, 2022[85])). But children may be at heightened risk given that, in some countries, the vast majority of children play video games (e.g. 86% of 9–18-year-olds in Norway (Forbrukerrådet, 2022[85])) and that children may often lack impulse control and an understanding of costs and manipulative techniques (see Box 2 below). For example, survey data indicate 55% of boys aged 15–16 in Norway had paid for loot boxes and 44% of 11–16-year-olds in the United Kingdom who were aware of loot boxes had spent money on them (Gambling Commission, 2019[86]; Medietilsynet, 2020[87]).

Box 2. Children as consumers in the digital world

Children have often been regarded as a vulnerable consumer group as they lack experience as consumers and are less able to resist the influence of others (Duivenvoorde, 2015[16]). An OECD typology of risks for children in the digital environment identified four specific kinds of risks children as consumers are exposed to online: i) marketing risks; ii) commercial profiling risks; iii) financial risks; and iv) security risks (OECD, 2021[56]). These risks can often be greater than the offline world: for example, evidence indicates online advertisements in websites and banner ads are harder for children to recognise than television advertisements (Kennedy, Jones and Williams, 2019[88]).

The gravity of such risks depends in part on a child's age. Research shows younger children do not comprehend the persuasive intent of advertising, appear to use fewer sources and less information when comparing and selecting products, and lack product knowledge and comprehension of pricing (Duivenvoorde, 2015[16]). Most research finds that unless children have a critical attitude to persuasion attempts, especially younger children cannot resist the persuasive influence of online advertising whether they recognise it or not (Kennedy, Jones and Williams, 2019[88]). Their overall literacy levels and comprehension skills are lower too, such that they may not understand the many disclosures they encounter online. As a result, they may be particularly susceptible to harm from online advertising and marketing practices where the persuasive intent is not clear, such as native advertising and endorsements in games and social media and dark patterns (see above). Yet children are also beginning to use the Internet, play online games and register on social networks at increasingly younger ages (OECD, 2019[89]; CNIL, 2020[90]).

Older children, in their teenage years, can in many ways have similar cognitive abilities to young adults, such that they may cope better with persuasion attempts (Duivenvoorde, 2015[16]). Some are more digitally capable than adults: in a survey of UK adults and children, the UK communications regulator (Ofcom) found children aged 14-15 had higher average confidence and understanding of digital communications and technology than all adult age groups (Ofcom, 2014[91]). Accordingly, it is important to consider a child's age, maturity and circumstances when considering a child's vulnerability as a consumer. Nonetheless, older children still have less experience as consumers than adults and may often exhibit more risky behaviour, because of limited impulse control (Steinberg, 2007[92]). This may mean they focus more on immediate gains than future costs (Steinberg, 2007[92]) and thus are more susceptible to addiction and financial loss in games, such as through micro-transactions and other in-game purchases (see above). As a result of their inexperience, children are also less aware of privacy risks in transactions involving personal data (OECD, 2021[56]).

Additionally, as with some adult consumers, some children may face additional difficulties in the digital environment in certain circumstances, such as children with disabilities, children from a minority racial or ethnic background, refugee children, children in care, LGBTQI+ children, as well as children with a disadvantaged socio-economic backgrounds (EC, 2022[93]).

Proliferation of dark commercial patterns

"Dark (commercial) patterns" is an umbrella term referring to a wide variety of practices in online user interfaces which, often by exploiting common cognitive and behavioural biases, steer, deceive, coerce, or manipulate consumers into making choices, e.g. regarding purchases, their personal data or time spent on websites, that may not be in their best interests. In its background report on the topic, the CCP proposed the following working definition 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" (OECD, 2022[3]).

E-commerce websites and apps (including children's apps), particularly those of major online platforms and marketplaces, often feature more than one dark pattern. Dark patterns also feature commonly in online games (particularly in the design of loot boxes), browsers and search engines as well as a significant proportion of cookie consent notices – the latter potentially entailing high rates of violation of data protection laws. The relatively more frequently encountered types of dark patterns on e-commerce websites and apps involve creating a false sense of urgency (through potentially misleading countdown timers or low-stock messages); generating social proof (through potentially misleading notifications of other consumers' activities or testimonials); using framing to privilege specific actions from the consumer favourable to the business (by preselecting options by default, giving them visual prominence, hiding information or disguising advertisements); forcing the consumer's registration for a purchase or disclosure of data; nagging the consumer repeatedly to make a choice; or making it difficult to cancel a service or opt out of settings (OECD, 2022[3]).

Given online businesses' ability to repeatedly run experiments and leverage data collected to hone user interface designs, consumers' heightened susceptibility to deception online (see above), as well as the scale of consumers reachable online, dark patterns are likely to be of greater cause for concern than analogous practices in brick-and-mortar stores. Various behavioural experiments have illustrated the potential for dark patterns to affect large shares of consumers. One study showed that when prices and information relating to deals regarding different broadband packages were dripped over multiple screens rather than displayed at once, 53% of consumers were unable to select the optimal deal (EC, 2016[25]). Another study found that 41.9% of consumers exposed to a series of "aggressive" and "mild" dark patterns accepted a hypothetical dubious identity and data protection program – a rate around four times higher than that of a control group exposed to no dark patterns (Luguri and Strahilevitz, 2021[94]).

In addition to impairing consumer autonomy, the harms that may result from dark patterns include financial and privacy loss, psychological detriment (including addiction), as well as weaker competition and loss of consumer trust at the collective level (OECD, 2022[3]). Evidence also indicates that some subsets of consumers are disproportionately affected. For example, Luguri and Strahilevitz (2021[94]) and a 2022 EC study on dark patterns and manipulative personalisation practices ("the 2022 EC study") (EC, 2022[95]) both found dark patterns to be more effective on older age and less educated consumers, and the latter also found them more effective on consumers in a situation of transitory vulnerability as a result of time pressure to make a choice. In a similar vein, Bongard-Blanchy et al. (2021[96]) found that both people over 40 as well as people possessing only high school diplomas were less likely to recognise dark patterns. In contrast, the CPRC (2022[97]) 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. Children are also likely to be particularly prone to be affected by dark patterns featuring in advertising in apps (Meyer et al., 2019[98]; Radesky et al., 2022[99]) and in online games to enhance monetisation (e.g. through loot boxes) (Bell and Fitton, 2021[100]). Consumers of lower socio-economic status may also be more affected. For instance, Radesky et al. (2022[99]) found children of families of low socio-economic status were more likely to encounter manipulative design features in children's apps. US tax software company TurboTax was also 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.[11] Further information on the prevalence, effectiveness in influencing consumer decisions and harms of dark patterns is detailed in the CCP's report on the topic (OECD, 2022[3]).

Growing potential for exploitative data-driven personalisation practices

Consumers' interaction with online businesses is mediated through Internet-connected devices, which allows businesses to collect highly granular information about consumers' online behaviour in order to personalise their online experience (Spencer, 2020[101]; Calo, 2014[102]; OECD, 2019[51]). With the development of sensor-equipped smart devices and advanced data analytics, businesses can also increasingly rely on observed and inferred data – unlike pre-digitalisation times when most business models fundamentally relied on data volunteered by consumers (OECD, 2015[103]; OECD, 2018[104]). The processing of these data through algorithms allows for fine-grained consumer profiles to be developed,[12] which are claimed to allow businesses to make predictions about a vast range of different aspects of consumers, including identity, resources, needs, habits, moods, behaviour, responses to stimuli, values and opinions (Willis, 2020[47]; Helberger et al., 2021[13]; Hirsch, 2020[105]). Third-party businesses also increasingly provide "predictive marketing" services combining different aspects of marketing and advertising technology, data, analytics, and profiling (Christl, 2017[106]). Data-based predictions based on consumer profiling in turn allow the online consumer experience to be further personalised (or individualised).[13]

Personalisation can influence consumer behaviour through specific psychological mechanisms, such as the greater salience of a personalised message and its enhanced credibility (CMA, 2022[107]). Possible benefits include online experiences that are more tailored to consumers' needs or preferences, reduced information overload, increased user engagement and satisfaction and greater convenience (CMA, 2022[107]). But some scholars submit that personalisation reflects a new form of information asymmetry, where businesses know much more about the consumer than vice versa. It is argued that consumers' lack of knowledge about such practices can make consumers vulnerable (Strycharz and Duivenvoorde, 2021[108]). Indeed, research shows that some consumers, such as those with financial difficulties or less education, may be less aware of personalisation than others (EC, 2018[109]). But it is also argued that such information asymmetry creates a transactional advantage allowing businesses to exploit not only generally known cognitive biases and dispositions (as many dark patterns do), but also the situational and idiosyncratic vulnerabilities of consumers at the individual level (Mik, 2016[110]; Helberger et al., 2021[111]; OECD, 2018[78]; OECD, 2015[103]; Strycharz and Duivenvoorde, 2021[108]; Calo and Rosenblat, 2017[112]). As with dark patterns, scholars suggest that such practices may undermine consumer autonomy and induce consumers to make choices against their best interests, potentially resulting in financial loss, privacy harms, psychological detriment, weaker or distorted competition and reduced consumer trust (Calo, 2014[102]; Zarsky, 2019[113]).

However, evidence of the prevalence, effectiveness of and detriment resulting from exploitative personalisation practices is still emerging; existing evidence appears in large part anecdotal or speculative in nature (see below). The following discussion explores how key forms of online personalisation – regarding advertising, pricing, rankings and digital choice architecture more broadly (i.e. in the form of dark patterns) – may have the potential to exploit consumer vulnerabilities.

Targeted advertising

Targeted advertising exists in various forms. Contextual advertising involves tailored banner ads based on content currently being viewed or searched. Demographic or segmented advertising is based on demographic information provided by consumers, such as age or gender. Behavioural advertising involves collecting data on consumers' online behaviour, such as their browsing history and location, to build detailed profiles in order to deliver targeted advertisements tailored to consumers' predicted interests (Boerman, Kruikemeier and Zuiderveen Borgesius, 2017[114]; Paterson et al., 2021[115]);[14] some commentators have referred to the practice as "surveillance advertising" (Forbrukerrådet, 2021[116]). A 2018 EC study found evidence of widespread usage of targeted advertising on European e-commerce websites (EC, 2018[109]).

Targeted advertising has the potential to provide two key benefits to consumers (OECD, 2019[51]). One is more relevant and timely ads, which can contribute to reduced search costs, greater awareness of relevant products, and identification of and access to deals. Second, online advertising funds a host of online services that consumers can access at zero (monetary) price, such as "free" search, social networking and news services. Marketers may be willing to pay more the more advertising is targeted, which could in turn fund higher quality zero-price services.

But there are some emerging cases and studies showing how targeted advertising may be used to exploit consumers' transitory or persistent vulnerabilities. For example:

- A marketing study purported to show that women felt less attractive on Monday mornings and recommended that companies focus on selling beauty products to women at that time (Rosen, 2013[117]; Calo, 2014[102]).
- A retail department store was able to determine which of its female customers were pregnant based on their purchasing histories and sent them coupons related to baby products (Hirsch, 2020[105]).[15]
- Advertising platforms were found to serve ads for casinos to consumers seeking advice about or attempting to stop gambling (Satarino, 2021[118]; Fletcher et al., 2021[77]).
- A social media platform was found to offer advertisers the opportunity to target teenagers at times they felt insecure (Spencer, 2020[101]; Tiki, 2017[119]) or children interested in smoking, alcohol and weight loss,[16] and to use sophisticated algorithms to target consumer groups that may bear health-related vulnerabilities (Bol et al., 2020[120]).
- A manufacturer of addictive painkillers was found to use data-matching techniques to track consumers' health-related searches and target them with ads in increasing frequency until they responded.[17]

Other studies show that online advertising can target behavioural traits associated to sensitive topics related to health, politics or sexual orientation (Carrascosa et al., 2014[121]) and that personality traits and psychological characteristics, such as impulsiveness, can be accurately inferred (e.g. from digital footprints, such as "likes" on a social media platform) and targeted to make advertising more effective (Matz et al., 2017[122]; Spencer, 2020[101]; Strycharz and Duivenvoorde, 2021[108]; Hirsch, 2020[105]), as exemplified in the Cambridge Analytica scandal.[18] Moreover, consumer survey data from several countries show that most consumers are uncomfortable with targeted advertising using personal data and tend to fear manipulation (Strycharz and Duivenvoorde, 2021[108]; Turow et al., 2011[123]; Forbrukerrådet, 2021[116]).

Yet the extent of targeted advertising exploiting vulnerabilities at a highly granular level is unclear. Previous CCP work indicated no evidence of online advertising targeting transitory or persistent vulnerabilities at scale (OECD, 2019[51]). Mystery shoppers in the 2022 EC study also did not consider targeted advertising identified on European e-commerce websites to be unfair or manipulative (EC, 2022[95]). Furthermore, evidence regarding the effectiveness and efficiency of targeted advertising is mixed. One study found the click-through rate (i.e. the proportion of an ad's total viewers who click on it) of behaviourally targeted advertising to be 5.3 times higher on average than advertising that does not use behavioural data (IHS Markit, 2017[124]). But other evidence indicates some forms of targeted advertising can be ineffective or inefficient (Williams, 2022[125]; Neumann, Tucker and Whitfield, 2019[126]), including when based on personality prediction (Marengo and Montag, 2020[127]) or psychographic targeting (Martinez, 2018[128]) methods.[19]

Nonetheless, some scholars expect that with ever greater data collection and improvements in AI techniques, marketers will increasingly be able to identify and further exploit biases and vulnerabilities with greater accuracy, in different ways (Spencer, 2020[101]). Emerging techniques include persuasion profiling,[20] involving use of fine-grained psychographic profiling to deliver the right advertising at the right time and place to the consumer (Helberger et al., 2021[111]; Calo, 2021[129]), and morphing, involving dynamically modifying an advertisement in real time to suit the consumer (Spencer, 2020[101]; Calo,

2014[102]; Christl, 2017[106]). Scholars suggest AI could learn to exploit vulnerabilities without any specific human command and even if a task has been neutrally defined, such as "*display the ad to X persons with the highest possibility of clicking, at the moment when the chance is the biggest*" (Jabłonowska et al., 2018[130]). Scholars also consider AI offerings will increasingly be able to target mental states such as emotions (Hacker, 2021[131]; Helberger et al., 2021[111]); indeed a number of major technology companies have already filed patent applications for technologies that dynamically detect moods or physiological states (Spencer, 2020[101]; Fussell, 2018[132]; Mahdawi, 2018[133]).

Personalised pricing

Personalised pricing, also known as first-degree price discrimination, is the practice of charging consumers based on their personal characteristics and conduct, resulting in each consumer being charged a price that is a function – though not necessarily equal – to his or her willingness to pay (OECD, 2018[104]). Evidence of personalised pricing is still emerging; studies have found it hard to find evidence of actual cases (OECD, 2018[104]; CMA, 2018[134]). EC studies in 2018 and 2022 found little evidence of the practice on European e-commerce websites (EC, 2018[109]; EC, 2022[95]). A 2021 study funded by the German Federal Ministry of Justice also found no evidence of personalised pricing on German e-commerce websites (ibi research & trinnovative, 2021[135]). There appears to be more evidence of online segmented pricing, i.e. charging different groups of consumers different prices, also known as third-degree price discrimination. For example, a recent study across six countries found significant use of segmented pricing in an online dating app, particularly on the basis of age, with participants aged 30-49 paying on average 65% more than those aged 18-29 (CI and Mozilla, 2022[136]). Nonetheless, some research indicates the business gains from personalised pricing could be significant, with studies indicating potential increases in business profits of 12% (Shiller, 2014[137]) or 19% (Dubé, Booth and Misra, 2022[138]). Hence market forces may push businesses to further take up personalised pricing in due course (Wagner and Eidenmüller, 2019[139]), especially with improvements in data collection and algorithms (CMA, 2018[134])

Personalised pricing can benefit consumers with a lower willingness to pay through lower prices, though those who have a higher willingness to pay, or are less discerning, lose out (OECD, 2018[104]). Specifically, when pricing is identical for all consumers, disengaged consumers who do not shop around benefit from the downward pressure on prices applied by those who do, but become more susceptible to losing out from higher prices when they are personalised (Wagner and Eidenmüller, 2019[139]). Consumer surveys also indicate most consumers find online price discrimination unfair and unacceptable (Poort and Borgesius, 2019[140]). And in some cases, personalised pricing may allow specific vulnerabilities to be exploited, which for some commentators amounts to a form of "data-driven coercion" (Christl, 2017[106]). For example, while it did not use the information to set prices, a ride-sharing service found that consumers with low mobile device battery were more likely to pay surge prices for a ride, seemingly out of anxiety of a dying battery (Vedantam and Penman, 2016[141]; Spencer, 2020[101]).

Personalised ranking of offers

Personalised ranking of offers, also known as search personalisation, relates to changing the order of search results to highlight certain goods and services, often based on navigation history, location and identified interests, but without changing the prices of offers (EC, 2018[109]). Similar to personalised pricing, evidence of personalised ranking of offers is still emerging. A 2018 EC study on online personalisation found that over three fifths of 160 e-commerce websites visited in the study personalised the ranking of offers (EC, 2018[109]). But the extent of personalised ranking exploiting vulnerabilities at a highly granular level is unclear; similar to targeted advertising, mystery shoppers in the 2022 EC study did not consider personalised ranking of offers identified on European e-commerce websites to be unfair or manipulative (EC, 2022[95]).

Similar to targeted advertising, personalised ranking can benefit the consumer by displaying more prominently an offer that suits a consumer's interests. However, similar to personalised pricing, the ranking of offers can also be tailored to extract consumers' maximum willingness to pay. Furthermore, personalised ranking can exploit position bias, i.e. consumers' tendency to disproportionately select top search results driven by a perception that a product is of higher quality because it is higher in the ranking (CMA, 2017[142]; ACM, 2021[143]).

Personalised dark commercial patterns

The dark patterns documented in the literature to date operate in the same way to all consumers, irrespective of their personal attributes or behaviours, i.e. they are not personalised. Scholars have not identified evidence of much use of personalised dark patterns, in the sense of personalised user interface designs that *"push each user's specific buttons"* (Narayanan et al., 2020[144]). They have speculated that this is because *"companies are busy picking lower-hanging fruit, but this can change any time."*

Nonetheless, some researchers suggest that, over time, larger volumes of data collected combined with machine learning techniques increasingly will enable businesses to personalise digital choice architecture for consumers (Willis, 2020[47]) including at a highly granular, individual level (which has been termed "hypernudging" (Yeung, 2017[145])). Willis (2020[47]) further suggests that the distinction between dark patterns and micro-targeted deceptive marketing may become illusory as today online marketing materials and sales interfaces are both *"created by machines optimised for business profit"*, noting that *"marketing today means maximizing selected business metrics, whether that be accomplished through statements, omissions, photos, information placement, or interactive webpage elements."*

Accordingly, some commentators suggest some forms of personalised dark patterns are likely to emerge (Willis, 2020[47]; Weinzierl, 2020[146]; Helberger et al., 2021[111]), including personalised drip pricing (CMA, 2021[147]) or time-limited offers (CMA, 2022[107]), which may be more effective than non-personalised dark patterns. Similar to other personalisation practices, scholars suggest personalised dark patterns could potentially be used to target specific subsets of consumers, such as those living in a certain area (e.g. residents of a retirement village, or people from different language backgrounds) or suffering from a specific health-related issue (e.g. mental illness). It is also suggested that they could be used to target consumers' vulnerabilities with a high level of granularity, such as individual consumers in a specific emotional or physiological state (e.g. bereavement or tiredness), including by serving them the specific dark patterns they are likely to be most susceptible to (Luguri and Strahilevitz, 2021[94]; Helberger et al., 2021[111]; Stigler Committee, 2019[148]; Willis, 2020[47]). Personalisation may also make it harder for consumers to identify when other dark patterns are being used, compounding their effects (CMA, 2022[107]).

Increasing risks of biased and discriminatory algorithms

Online businesses increasingly use algorithms to automate decision-making and processes in their dealings with consumers. Many algorithmic systems provide substantial benefits to consumers, including through automated access to and continuous improvement of products and services (CMA, 2021[147]), as well as through personalised goods and services (as discussed above). Algorithmic systems also provide the potential to better protect consumers online, such as with AI-based web-crawlers that detect dark patterns, fake reviews and ratings or unsafe goods sold on websites (OECD, 2020[69]). [21]

But they may also raise risks involving bias and discrimination, whereby some consumers are disproportionately targeted, receive goods and services on less favourable terms or are excluded from them entirely. Such outcomes have been identified in particular in automated decisions regarding eligibility for or the favourability of terms regarding a range of services (e.g. insurance, healthcare or housing) as well as exposure to advertising (Christl, 2017[106]), and may become more common with greater business usage of algorithms. In addition, as algorithms often operate opaquely for consumers, without their necessarily having consented to them, grounds to seek redress may often be unavailable. As with

exploitative personalisation practices, however, robust evidence regarding the current scale of discriminatory or biased algorithms and the associated detriment is yet to emerge.

Discriminatory consumer outcomes can occur in several ways. One is where algorithmic systems make decisions that directly treat consumers differently based on certain legally defined "protected characteristics", such as gender (see e.g. Datta, Tschantz and Datta (2015[149])), age,[22] ethnic background, religion, political views, nationality, disability, sexual preferences or marital status. But another is indirect, i.e. where algorithms make decisions based on factors that are correlated in some way with certain protected characteristics and thus have disparate impacts on consumers with such characteristics, without that necessarily being the intent (OECD, 2019[150]).[23] For example, when in 2016 an online marketplace expanded its same-day delivery service in the United States, it focused on areas with high concentrations of existing subscribers to the service. As a result, however, predominantly black neighbourhoods were excluded, despite the areas surrounding those neighbourhoods being served (Ingold and Soper, 2016[151]; CMA, 2021[147]). Similarly, in several countries, algorithms have been found to charge consumers living in certain postcodes more for car insurance, e.g. because accidents in such postcodes may be more frequent, though they can often also be low-income neighbourhoods.[24] Other studies have identified discriminatory outcomes regarding exposure to advertising, such as in search queries (Sweeney, 2013[152]) and on social media platforms (Zang, 2021[153]; DQUBE Solutions et al., 2020[154]; Bol et al., 2020[120]), when the algorithms involved are based on factors such as racially stereotypical names, postcodes, pre-defined advertising categories or societal stereotypes. The correlating factor may also be unclear or appear neutral: for example Ali et al. (2019[155]) found that despite setting equal and highly inclusive targeting parameters in the algorithms governing a social media platform's ad delivery processes (which seek to optimise according to a chosen outcome such as most clicks or views), there was nonetheless substantial gender and racial bias.

Another way algorithmic systems can be indirectly discriminatory is if they use and train themselves on consumer data that are inaccurate, incomplete or outdated or on data that reflect historical biases and inequalities. In that case, such inaccuracies and biases will likely carry through to the way in which the algorithm operates and the outcomes it generates. Systemic use of such algorithms may in turn replicate existing biases and exacerbate marginalisation of certain groups and societal stereotypes and inequalities (OECD, 2019[2]; Paterson et al., 2021[115]; Lee, Resnick and Barton, 2019[156]).

Continuing digital divides

In many countries, there remains a "digital divide", i.e. different levels of access to and use of information and communication technologies (ICTs), including Internet-based digital services (OECD, 2018[157]). Specifically, in 2020, the proportion of adults accessing the Internet ranged from over 99% to less than 74% among OECD countries. Less or lack of access hinders consumers' ability to effectively engage in e-commerce and reap the benefits of the digital transformation. Moreover, depending on the country, the divide may affect certain consumers more than others. For example, 58% of consumers aged 55-74 used the Internet frequently in 2019 – up from 30% in 2010, but still well below the share for daily users aged 16-24, which was close to 95%. In 2018, only 40% of adults in OECD countries with low or no formal education used the Internet to interact with public authorities, compared to 80% of those with tertiary education (OECD, 2020[69]). In Australia, for example, specific consumer groups remain less digitally included than others, including those on low incomes, the elderly, unemployed, disabled, and those living in rural areas (CPRC, 2020[158]).

One cause of the digital divide is a gap in connectivity. For example, in 2019, only 59% of rural households in Europe were located in regions where access to fixed broadband with a minimum speed of 30 Mbps was available, in comparison to 86% of households in all areas (OECD, 2021[159]). But another key cause is differences in digital skills and literacy, especially as people with greater skills can make better use of the Internet and online activities (OECD, 2021[159]). In some countries, the share of Internet users

performing relatively more complex activities online, such as e-banking, online purchases, news reading and use of government services (e-government), is substantially lower than it is for simple activities (OECD, 2020[69]). Certain socio-demographic characteristics are also correlated with different types of online activity. In Japan, 42% of consumers over 70 who do not use digital devices on a daily basis considered smartphones and tablets were too difficult to use (CAO, 2020[160]), and in Canada, seniors were found to have the lowest levels of digital access and skills.[25] In OECD countries, rural areas have a lower share of individuals with at least basic digital skills than in cities (OECD, 2021[159]). Numeracy skills also affect digital skills and literacy. One study found less than 10% of European consumers who use the Internet mainly for information and communication had good literacy and numeracy skills (OECD, 2020[69]); another report suggested that around half of UK adults had the numeracy level that would be expected of primary school children (National Numeracy, 2021[161]).

In turn, lack of digital skills and literacy and numeracy skills may also make consumers particularly vulnerable to harm from certain online marketing practices, such as those involving complex terms and conditions or pricing practices (FCA, 2015[29]).

Implications for consumer policy and law

A possible new conceptualisation of consumer vulnerability in the digital age

Each of the trends highlighted above illustrate how, in different ways, the scale and nature of consumer vulnerability in the digital age appear to be changing. A key insight is that vulnerability is not necessarily experienced only by certain subsets of consumers. Rather, it may increasingly be experienced by the vast majority of, if not all, consumers, at different times and depending on the role of various market factors – even if some consumers may continue to experience it disproportionately.

Many scholars and other stakeholders have accordingly called for a new conceptualisation of consumer vulnerability in the digital sphere, according to which digital vulnerability is "universal" or "systemic" and where all consumers could be vulnerable depending on the circumstances (Mik, 2016[110]; Fletcher et al., 2021[77]; Helberger et al., 2021[13]; Riefa, 2020[26]; Calo, 2014[102]; Forbrukerrådet, 2021[116]). To reflect this, Siciliani, Riefa and Gamper (2019[75]) for example, prefer the notion of "consumers in vulnerable situations" to "vulnerable consumers". In characterising digital vulnerability, Helberger et al. (2021[13]) place particular emphasis on its architectural and relational nature, in consideration of the role of businesses' digital choice architectures and their dynamic, asymmetric relationship with consumers, as well as how lack of privacy reinforces such vulnerability. Scholars have also highlighted that various economic or social inequalities could be entrenched or exacerbated along a number of fault lines as a result of the trends described above – such as technological know-how, digital inclusion, cognitive bias or impairment, tendency to be subject to discrimination (Bol et al., 2020[120]) and the balance of power between large online businesses and consumers (Helberger et al., 2021[13]).

Such a conceptualisation largely aligns with the broad state-based approach to consumer vulnerability reflected in the 2014 OECD Recommendation on Consumer Policy Decision Making, as described above. The external factors it lists are the characteristics of the market for a particular product; the product's qualities; the nature of a transaction; and the internal factors are the consumer's attributes or circumstances. As the discussion of trends highlights above, these factors continue to be relevant in today's digital transformation. Specifically:

- E-commerce or digital *markets characterised* by lack of competition, information asymmetries, obfuscation, bargaining power imbalances, network access deficiencies, or a high prevalence of dark patterns and exploitative personalisation practices may make consumers more vulnerable.

- Specific *qualities* of digital or e-commerce products, particularly new technologies, can exacerbate consumer vulnerability, such as the complexity of associated disclosures or their levels of safety or data privacy.
- Consumers with less experience with certain kinds of online *transaction* may be exposed to greater detriment, such as financial loss (e.g. auto-renewing subscriptions), privacy loss (e.g. non-monetary transactions), or addiction (e.g. in-game transactions).
- Finally, certain *attributes or circumstances* may make some digital consumers more susceptible to detriment in certain contexts, either on a transitory basis or persistently. These include cognitive impairment or poor computational skills, native language limitations, low digital literacy, low literacy or numeracy, physical disabilities (such as visual impairment), and other structural inequities (e.g. unequal access to resources or opportunities) (OECD, 2010[1]). Personality-based characteristics considered to exacerbate vulnerability include being credulous, impulsive, risk averse or being less trusting of people (EC, 2016[25]). Relevant personal circumstances could include going through a bereavement, a divorce, or a period of illness (CMA, 2019[27]).

Accordingly, the 2014 Recommendation's conceptualisation of consumer vulnerability continues to be broadly relevant in the digital age and act as an appropriate basis for developing policies to address consumer vulnerability. This is supported by the CCP's 2019 review of the implementation and impact of the Recommendation, which found it "*remains highly relevant and does not require any change at this stage"* (OECD, 2019[162]). As discussed above, recent policy research and guidance shows that several jurisdictions have, in effect, adopted a state-based approach to vulnerability that could equally serve as a starting point to addressing vulnerability-related challenges brought about by the digital age.

Possible implications for consumer law in some jurisdictions

Some jurisdictions have begun to anchor a broader view of consumer vulnerability in the law. Simpson (2020[36]), for example, considers that "*the legislative pendulum has swung away from a system based on freedom of contract, with some defined exceptions, towards a more generic principle of assuming a wide degree of vulnerability with some consumers requiring particular attention over and above a baseline".* The Brazilian Consumer Defence Code, for example, regards all consumers as vulnerable by definition. A number of jurisdictions have furthermore established the concept of "hypervulnerable" consumers in law or guidance, to characterise vulnerabilities that may be more acute than a base level of "structural" vulnerability applying to all consumers (see Table 1, Section 2, for more details on laws in different jurisdictions defining or classifying vulnerable consumers).

But it has been argued that a broader conceptualisation of consumer vulnerability is not necessarily reflected in the consumer law of certain jurisdictions that employ an "average" or "reasonable" consumer legal standard for the purposes of assessing potentially unfair or deceptive commercial practices (see Box 3 below for details on such standards).

Box 3. The "average" or "reasonable" consumer standard

Some jurisdictions employ an "average" or "reasonable" consumer legal standard (or "test") for the purposes of assessing potentially unfair or deceptive commercial practices. For instance, the EU Unfair Commercial Practices Directive (UCPD) provides that the unfairness of a practice shall be assessed by the impact it has on the "average consumer", similar to e.g. Quebec consumer law.[26]. The average consumer test concept in the European Union was developed by the European Court of Justice prior to the UCPD and codified in the UCPD (EC, 2021[163]). Similarly, the Federal Trade Commission (FTC) Act in the United States considers how a "reasonable consumer" would be affected by allegedly deceptive advertising or marketing (US FTC, 1984[164]),[27] and courts in Australia apply an "ordinary or reasonable consumer" test when assessing misleading or deceptive conduct (Corones et al., 2016[165]; Webb et al., 2020[166]).

The rationales for introducing such standards include to avoid placing disproportionate liability on businesses with respect to individual consumers for consumer harm and, in the European Union, to provide courts with common criteria and avoid disproportionate barriers to intra-EU trade. This is explained in guidance and court decisions of the relevant jurisdictions. Specifically, in explaining the "reasonable consumer" standard, the US FTC notes "*A company is not liable for every interpretation or action by a consumer"* and that *"certain practices […] are unlikely to deceive consumers acting reasonably. Thus, the [US FTC] generally will not bring advertising cases based on subjective claims (taste, feel, appearance, smell)"* (US FTC, 1984[164]). Similarly, in explaining the rationale for an "ordinary and reasonable" consumer test in Australia, the High Court of Australia held that *"The heavy burdens which the section [of consumer law prohibiting misleading or deceptive conduct] creates cannot have been intended to be imposed for the benefit of persons who fail to take reasonable care of their own interests." (1982) 149 CLR 191, 199)* (Corones, 2014[167]). EC guidance explains that the average consumer standard was codified "*to give national authorities and courts common criteria to enhance legal certainty and reduce the possibility of divergent assessments"* and that *"[harmonisation of EU consumer law through] the UCPD is based on the idea that, for instance, a national measure prohibiting claims that might deceive only a very credulous, naive or cursory consumer (e.g. 'puffery') would be disproportionate and create an unjustified barrier to trade."* (EC, 2021[163]).

In jurisdictions employing such standards, who the average or reasonable consumer is depends on who is targeted by the practice. If it is a particular subset of consumers, such as children interested in games, indebted consumers seeking a short-term loan or terminally ill consumers seeking specific medicine, then the assessment of the legality of the practice is based on the perspective on an "average" or "reasonable" consumer of that group (US FTC, 2021[168]; Corones, 2014[167]; ACM, 2020[169]). By the same token, a practice such as a prescription drug advertisement directed at doctors would be judged in consideration of the knowledge and sophistication of that group (US FTC, 1984[164]).

If a practice is targeted at consumers in general, then an average or reasonable consumer of the general population is the benchmark. In some cases, such a consumer might be understood to be different from a "vulnerable" consumer. In the UCPD, for example, the average consumer is understood to be *"reasonably informed, circumspect, and observant consumer, taking into account social, cultural and linguistic factors"* (Recital 18)[28]. This is distinguished from a "vulnerable" consumer, whose vulnerability under the directive may only result from a few personal attributes – namely, infirmity, age or credulity (Art 5(3)). Nonetheless, depending on how the standard is employed in different jurisdictions, the average or reasonable consumer may well be considered particularly vulnerable to some practices. For example, the US FTC clarifies that "*the test is whether the consumer's interpretation or reaction is reasonable",* noting that "*reasonable consumers do not read the entirety of an ad or are directed away from the importance of the qualifying phrase by the acts or statements of the seller",* and could thus be vulnerable to practices that seek to hide important information disclosures (US FTC, 1984[164]).

Specifically, researchers have questioned from several perspectives the way the average or reasonable consumer is understood, as distinct from a vulnerable consumer, and the continued relevance of such standards. First, many scholars consider that such standards depict an overly rational and informed consumer with insufficient regard for cognitive biases and vulnerabilities that may be exploited, and find that courts in the European Union and United States, for instance, have tended to follow this understanding (Duivenvoorde, 2015[16]; Cohen, 2019[170]; Riefa and Gamper, 2020[171]). Some researchers submit that the UCPD, which defines both an average consumer and a vulnerable consumer (see Box 3 above), leaves a gap in consumer protection by failing both to protect consumers falling below the average standard and to recognise vulnerability arising from situational circumstances rather than personal attributes (Howells, Twigg-Flesner and Wilhelmsson, 2017[172]; Strycharz and Duivenvoorde, 2021[108]; Kaprou, 2020[7]).

Other commentary considers that the potential for today's digital practices to affect all consumers' vulnerabilities, potentially at an individual level, implies a much narrower gap between an average consumer and a "vulnerable" consumer. For instance, a 2017 EC evaluation of the UCPD ("the 2017 EC evaluation") found that online practices that target consumers' specific biases *"are likely to specifically affect vulnerable consumer groups but also consumers that could be considered to be a closer match to the concept of an 'average consumer'"* (EC, 2017[173]). In the same vein, Helberger et al. (2021[13]) argue that in digital markets, not only is the vulnerable consumer no longer the exception, but the ordinary or average consumer is no longer the rule, and is as such an "unrealistic prototype". Researchers further argue that because data-driven personalisation practices may target a single consumer at a single moment in time and space, potentially when they are most vulnerable, there is no longer a distinction between the actual consumer and the average or reasonable consumer, making the standard of little practical use (Willis, 2020[47]; Micklitz and Namyslowska, 2020[174]).

Several consumer organisations and some consumer authorities have accordingly recommended a move away from the average consumer benchmark in the European Union (BEUC, 2022[175]; EC, 2017[173]). Some researchers have also proposed specific consumer law reforms that may entail less reliance on such standards (Siciliani, Riefa and Gamper (2019[75]) and Willis (2015[176]); see further discussion in Section 2). In some sectors, the "notice and choice" framework, which assumes a baseline average consumer who can benefit from privacy notices, is also falling out of favour (US FTC, 2010[177]).

Yet there are several reasons to exercise caution in revisiting such standards. First, the definitive characteristics of an average or reasonable consumer may not yet be fully understood and may require more evidence. Specifically, the 2017 EC evaluation considered that obtaining a realistic picture of an average consumer may require further, potentially case-specific, empirical insights (EC, 2017[173]). Indeed, based on consumer survey data the 2016 EC vulnerability study found that for each of the dimensions of vulnerability it identified (see above), the "average consumer," if understood as providing the median response to the survey, *"exhibits few signs of vulnerability"* and *"appears to be well informed (although not too thorough in reading communication from providers) and circumspect*" (EC, 2016[25]).

Second, such standards may be flexible to case-specific interpretations, which could help reflect a broader understanding of vulnerability. As discussed in Box 3 above, a reasonable consumer may well be one that does not fully read relevant disclosures (US FTC, 1984[164]). The EU average consumer standard has also been adjusted to the circumstances of specific cases and does not necessarily preclude adopting a more realistic understanding of an "average" consumer reflecting findings of behavioural science, as courts in some Nordic countries have done (EC, 2017[173]); indeed EC guidance recommends that courts and authorities assess commercial practices by taking into account the most recent findings from behavioural economics (EC, 2021[163]). In the same vein, the Supreme Court of Canada ruled in a case under Quebec's Consumer Protection Act that an average consumer is an ordinary, hurried, "credulous and inexperienced consumer" who is not particularly experienced at detecting the falsehoods or subtleties found in commercial representations.[29] Likewise, the Federal Court of Australia has suggested that an "ordinary or reasonable" member of the target audience of advertising may be one who reads the advertising fleetingly, is somewhat gullible and not wary, and not necessarily well-educated or digitally literate.[30] Cohen

(2019[170]) similarly suggests a less sophisticated interpretation of the reasonable consumer could apply in US courts. Moreover, both the EC and the ACM have clarified in guidance that if a practice is personalised to the level of a single consumer, that consumer can be considered the average consumer for the purposes of the UCPD (ACM, 2020[169]; EC, 2021[163]). Existing legal notions of vulnerable consumer may also be amenable to more nuanced interpretation; the recently revised EC guidance on the UCPD clarifies that its concept of vulnerability is indeed dynamic and situational, meaning, for instance, that a consumer can be vulnerable in one situation but not in others (EC, 2021[163]).

Finally, departing from such standards could risk compromising the objectives they sought to deliver discussed in Box 3 – namely by potentially placing disproportionate liability on businesses with respect to individual consumers, and, in the European Union, creating disproportionate barriers to intra-EU trade. As noted by Cohen (2019[170]), legal standards may need to strike a balance between competing priorities, since *"a rule that consumers are always deceived by exploitative practices would maximize certainty at the expense of commerce".*

On the whole, therefore, even if a broader consideration of consumer vulnerability is adopted in consumer policy and parts of consumer law, more evidence on whether existing legal standards used in some jurisdictions continue to be appropriate in the digital age nonetheless appears warranted. Still, if most if not all online consumers could be considered vulnerable at certain times, the dividing line between policies to address digital consumer vulnerability and to improve consumer protection online in general is blurred. Helberger et al. (2021[111]) note, in this regard, that *"addressing vulnerability and bringing fairness into the digital marketplace is not simply a question of empowering consumers, but of changing markets"*. This points to broader questions about digital consumer policy, with the consideration that addressing digital consumer vulnerability and protecting consumers online in general could, at least in the longer term, ultimately be the same objectives – even if certain consumers may continue to warrant specific attention in specific circumstances (as further discussed below).

2 Measures to address consumer vulnerability in the digital age

Many jurisdictions have implemented measures to address the vulnerability of specific subsets of consumer groups. This follows from the general principle that measures that may empower or protect consumers in general may be insufficient for specific consumer groups, who may require more targeted measures. A case in point is information disclosures: the European Parliament (EP), for example, recognised that focusing on information and education "*may be insufficient to protect vulnerable consumers, since their vulnerability may originate from their difficulty in accessing or assessing the information given to them"* (EP, 2012[178]; Siciliani, Riefa and Gamper, 2019[75]).

Yet, as noted above, it is increasingly the case that addressing consumer vulnerability online means improving consumer protection and empowerment across the board. In illustration of this point, the 2016 EC vulnerability study categorised measures to address consumer vulnerability by the drivers they focused on; some address the personal and demographic drivers of consumer vulnerability, while others address the behavioural, market-related, access or situational drivers of vulnerability.

Hence this section broadly reflects this dichotomy; it first discusses measures that seek to address the vulnerability of specific consumer groups online, followed by those addressing the vulnerability of consumers in general in the digital environment.

Measures addressing the vulnerability of specific consumer groups

A number of jurisdictions have developed measures that seek to address the vulnerability of specific consumer groups. Such measures can come in the form of targeted regulation or enforcement actions, guidance and awareness raising and relevant business initiatives, as described below. However, it is important to note that the effectiveness of such measures in alleviating consumer vulnerability may vary substantially. For instance, the 2016 EC vulnerability study found that measures addressing consumer vulnerability were relatively common across EU member states, with some having developed a broader national strategic approach. But no clear pattern emerged between the identified national measures and the incidence of vulnerability measured for each member state (EC, 2016[25]).

Measures targeting specific consumer groups understood as vulnerable

Some jurisdictions clearly define and/or provide special protective measures for a number of specific subsets of consumers understood as vulnerable in their legislation, which may apply in the context of particular online transactions or in general. Indeed, results of a survey of Consumers International (CI) members in 2020 showed that 60% of countries surveyed had a provision in law relating to "vulnerable consumers" (CI, 2021[179]).

Table 1. Examples of regulatory measures targeting specific consumers understood as vulnerable

Jurisdiction	Regulatory measures
Argentina	The Secretariat of Internal Trade adopted Resolution 139/2020 on "Hyper-vulnerable Consumers", which defines hyper-vulnerable consumers, describes some causes of hyper-vulnerability and provides instructions for relevant authorities to implement appropriate measures to protect them specifically. Article 3 of Draft Code No 5156/2020, legislation that was yet to pass at the time of writing, defines hyper-vulnerable consumers as consumers who, in addition to their structural vulnerability, are also in other situations of vulnerability due to their age, gender, health, or other social circumstances that make it particularly difficult to fully exercise their rights as consumers. The Article would require that in such cases, and within the framework of the consumption situation, education, health, information, fair and dignified treatment and safety must especially be guaranteed (FIAGC, 2021[180]).
Brazil	According to Article 4, I, of the Consumer Protection Code, all consumers are presumed vulnerable by definition. In addition, the Consumer Defence Code defines hyper-vulnerable consumers, who benefit from additional protections. Hyper-vulnerable consumers may include the elderly, children, people with disabilities, as well as women, in specific situations, either due to poverty or family overload (single-parent families). Furthermore, Article 39 prohibits exploiting the weakness or ignorance of a consumer that may relate to age, health, knowledge or social condition, in order to impose their products or services (FIAGC, 2021[180]).
Colombia	The law and constitution provide special protections to children and adolescents and older persons because of their special vulnerability as consumers (FIAGC, 2021[180]).
Costa Rica	In 2017, amendments were made to the Regulations for Law 7472 to require businesses to take special care to ensure that advertising aimed at minors, vulnerable or disadvantage consumers, and others who may not have the capacity to understand the information they are presented with, does not harm their dignity and well-being (UNCTAD, 2018[181]).
European Union member states	The UCPD, which prohibits unfair commercial practices, specifies that *"commercial practices that are likely to materially distort the economic behaviour only of a clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product 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 from the perspective of the average member of that group"* (Article 5(3)). The guidelines for the management of the EU Rapid Information System (Rapex) and its notification system (Commission Implementing Decision (EU) 2019/417 of 8 Nov.2018) establish definitions of "very vulnerable consumers" (children of age between 0 to 36 months and persons with extensive and complex disabilities) and "vulnerable consumers" (children older than 36 months and younger than 15 years, and persons with reduced physical, sensory or mental capabilities (e.g. partially disabled, elderly, including those over 65, with some reduction in their physical and mental capabilities), or lack of experience and knowledge. Furthermore, the Regulation on consumer online dispute resolution (ODR) requires that an ODR platform *"is accessible and usable for all, including vulnerable users ('design for all'), as far as possible"* (Article 5).
Israel	An amendment was made in 2016 to the Israel Consumer Protection Law such that a senior citizen, a person with disabilities or a new immigrant may cancel a distance selling transaction within four months from the date of the transaction, the date of receiving the product or the date of receiving the document containing the information specified in the law, whichever is later, provided the transaction included a conversation between the business and the consumer, including a conversation by electronic means. This contrasts with other consumers, who have a period of fourteen days.
Japan	In 2016 and 2018, the Consumer Contracts Act was revised to establish a rescission right from certain consumer transactions for certain groups of consumers, such as elderly people with dementia, consumers deemed unable to make reasonable decisions or young consumers who fall prey to dating and romance scams.
Korea	Article 45 of the Framework Act on Consumers requires the national and local governments to preferentially adopt measures to protect the "safety-vulnerable" population, understood as children, the elderly, the weak, persons with disabilities, and immigrants by marriage. It also requires that when selling, advertising, or offering goods, etc. to the safety-vulnerable population, businesses take necessary preventive measures to protect the safety-vulnerable population from any danger or injury.[31]
Mercosur member states	The Common Market Group of Mercosur Resolution of 36/2019 recognises the structural vulnerability of all consumers in the market and was to be implemented in legislation of Mercosur member states by 15 January 2020. Resolution 11/2021 on "Hyper-vulnerable Consumers", which was to be implemented by 15 January 2022, further defines hyper-vulnerable consumers as individuals with aggravated vulnerability, who are disadvantaged due to their age, physical or mental condition, or social, economic, ethnic and/or cultural circumstances, causing special difficulties to fully exercise their rights as consumers in specific acts of consumption they carry out. Mercosur member states must adopt a range of measures in relation to hyper-vulnerable consumers, including regarding dispute resolution, access to justice, guidance and advice, education, communication, access to information, promotion of good commercial treatment, protection from misleading and abusive offers, and protection of data and privacy. [32]
Peru	The Peruvian Consumer Protection Code, Article IV, paragraph 4, states that consumer protection should place special emphasis on those who are most likely to be victims of practices contrary to their rights, which include pregnant women, girls, children, elderly people and people with disabilities, as well as consumers in rural areas or in extreme poverty (UNCTAD, 2018[181]).
Spain	A definition of vulnerable consumer was incorporated into the General Law for the Defence of Consumers and Users by Royal Legislative Decree in 2021. The definition includes individuals who, individually or collectively, due to their characteristics, needs or personal, economic, educational or social circumstances, are territorially, sectorally or temporarily in a situation of subordination, defencelessness or lack of protection preventing the exercise of their rights as consumers equally to others (FIAGC, 2021[180]).
Republic of Türkiye	According to Articles 5-8, 9-15 of the Implementing Regulation on Commercial Advertising and Unfair Commercial Practices[33], no advertising shall include statements and images abusing sick people, children, elderly and disabled.

Source: Sources indicated in table.

Many jurisdictions also have sector-specific protections for certain subsets of consumers, which they may define as vulnerable, particularly in essential services such as electricity and water or the financial sector. While such services can often be signed up to online, as the measures are sector-specific and go beyond the digital environment they are beyond the focus of this report.[34]

Even where the law does not define or provide protective measures for specific subsets of consumers, investigation and enforcement actions are in practice often directed at certain consumer groups that consumer authorities understand as vulnerable or that are disproportionately affected by certain practices. For example, in France, in its surveillance activities of 2020 the Directorate General for Competition, Consumer Affairs and Fraud Control (DGCCRF) monitored the offers of products or services, including online, aimed more particularly at children, the elderly or consumers in a situation of particular fragility. As another example, the CMA took action against online gambling firms that made it difficult for customers to access their winnings and thus harder for them to stop gambling, and secured undertakings from firms to stop engaging in such practices (CMA, 2019[27]). More broadly, at the time of writing UNCTAD's World consumer protection map indicated that 49 countries had agencies that carried out initiatives for vulnerable and disadvantaged consumers.[35]

In some jurisdictions, regulatory authorities or self-regulatory bodies have also issued guidance regarding the steps businesses should take in relation to consumers understood as vulnerable. For example, in 2021 the ACCC and FCA issued guidance to assist businesses in complying with their obligations under relevant laws and encourage fairer treatment of consumers who may experience vulnerability (FCA, 2021[182]; ACCC, 2021[28]). In 2018, the Committee of Advertising Practice (CAP), a self-regulatory advertising body in the United Kingdom, issued guidance on how the Code of Non-broadcast Advertising and Direct & Promotional Marketing (CAP Code) seeks to assist consumers with vulnerability characteristics (CAP, 2018[183]). The International Organization for Standardization (ISO) in 2022 supplied such guidance at the international level, through a standard (ISO 22458:2022) for organisations on how to design and deliver fair, flexible and inclusive services to improve outcomes for consumers in vulnerable situations, covering organisational culture and strategy, inclusive design and how to identify and respond to consumer vulnerability (ISO, 2022[184]).

Measures targeting children as consumers online

Existing measures

In response to a 2017 OECD survey, only a few countries reported that their laws specifically addressed consumer risks for children (OECD, 2020[57]). Currently there is also no commonly accepted global approach to regulate the practice of commercial profiling of children (ICPEN, 2020[185]). In consideration of these findings, inter alia, the 2021 OECD Recommendation on Children in the Digital Environment recommended that national legal frameworks provide effective remedies for harms suffered by children in the digital environment, and that new measures be introduced if existing legal frameworks failed to protect children or provide effective remedies (OECD, 2021[23]). The Companion to the Recommendation further underlines that children merit special protection with regard to privacy and data protection, particularly owing to a lack of understanding of the commercial value of their data (OECD, 2022[186]). A 2021 comment from the UN Committee on the Rights of the Child (UNCRC) also encourages countries to make the best interests of the child a primary consideration when regulating advertising and marketing to children, including through prohibiting profiling or targeting of children and use of certain marketing techniques with children such as neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality (UNCRC, 2021[187]).

In recent years, several jurisdictions have put in place measures to regulate online commercial practices that specifically target or that otherwise affect children as consumers (Table 2 below), which may in some cases build on other provisions that define them and other subsets of consumers as vulnerable (as

discussed above). A particular focus has been on regulating online advertising directed at children, the collection and use of children's personal data and loot boxes in online games.

Table 2. Examples of regulatory measures addressing protection of children as consumers online

Jurisdiction	Regulatory measure
Belgium	In 2018, the Belgian gambling regulatory authority (Kansspelcommissie) came to the conclusion that loot boxes constituted a form of gambling under national legislation and they were hence banned from video games (Cerulli-Harms et al., 2020[188]).
Canada	The Consumer Protection Act Québec prohibits commercial advertising directed at children under 13 years of age in print and electronic media.[36]
Colombia	There are special provisions related to the right to information and publicity enjoyed by children and adolescents. These provisions also cover e-commerce (FIAGC, 2021[180]).
Costa Rica	According to executive decree No.40703 (October 3, 2017, in article 262), businesses have to adopt measures regarding online advertising to prevent minors from having access to goods and services that are not suitable for minors.
European Union member states	A direct exhortation to children to buy advertised products or persuade their parents or other adults to buy advertised products for them is prohibited under the UCPD, Annex I, No.28. A number of the UCPD's provisions may also apply in relation to protecting children in the context of disclosures of commercial communications on social media platforms, influencer marketing or in-game or in-app transactions. There are also specific rules under the GDPR regarding the validity of children's consent and the provision of information when information society services are offered directly to children (EC, 2021[163]).
Germany	The Youth Protection Act amended in 2021 obliges large providers of commercial Internet services for minors to provide appropriate and effective protection measures for minors. This includes deactivating "cost traps" such as loot boxes by default. (BMJV, 2021[189]). Targeted advertising to minors, including regarding loot boxes, is also subject to restrictions in Section 6 of the Interstate Treaty on the Protection of Minors in the Media, which states that advertisements must not harm the interests of minors and must not contain direct appeals to buy goods or services which at the same time exploit the inexperience and credulity of minors (Cerulli-Harms et al., 2020[188]).
Israel	The Consumer Protection Regulations (Advertisements and Marketing Methods Aimed at Minors) require that advertising and marketing, including online, must be compatible with the knowledge, understanding and maturity of the targeted audience and prohibits advertising or marketing that takes advantage of minors' innocence, beliefs, imagination and lack of experience (UNCTAD, 2018[181]).
Japan	In 2012, the CAA announced that use of loot boxes ("complete gacha"), would be subject to Orders for Action under Japan's Act against Unjustifiable Premiums and Misleading Representations and the Law for Preventing Unjustifiable Extra or Unexpected Benefit and Misleading Representation, such that loot boxes were de facto prohibited (Liu, 2019[190]).[37]
Korea	Existing laws regarding protection of children apply to games containing loot boxes (Leahy, 2022[82]).
People's Republic of China	A number of format-specific rules have been introduced governing loot boxes aimed to protect children, including spending limits, mandatory disclosure obligations for probabilities regarding contents, and rules on identification, registration and payment confirmation (Leahy, 2022[82]).
Republic of Türkiye	Implementing Regulation on Commercial Advertising and Unfair Commercial Practices[38] provides a comprehensive set of principles that should be followed regarding advertising directed at children or advertising where children are represented.
United States	The Children's Online Privacy Protection Act (COPPA) and the US FTC's COPPA Rule prohibit unfair or deceptive acts in the connection with the collection, use, or disclosure of personally identifiable information from and about children on the Internet, including by requiring websites to obtain verifiable parental consent prior to such data usages. The law applies to operators of commercial websites and online services (including online advertising) targeted at children under 13 years of age (OECD, 2019[191]).

Source: Sources indicated in table.

Consumer authorities in a range of jurisdictions have taken enforcement action to protect children from certain marketing practices online, such as the illegal marketing of goods and services to minors, misleading information to children regarding costs, or failing to obtain parental consent before using children's personal information (OECD, 2019[52]). More recently, consumer authorities in both the European Union[39] and the United States 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.[40]

Recent regulatory guidance also clarifies the scope of existing laws in certain jurisdictions pertaining to protection of children as consumers and their data online. For example, in France, the data protection authority (CNIL) published eight recommendations to reinforce the protection of minors online in regard to their personal information[41]. The UK Information Commissioner's Office (ICO) released an "Age

appropriate design code" containing 15 standards that online services should abide by to ensure compliance with their obligations under data protection law to protect children's data online (ICO, 2020[192]). In Germany, the Commission for Youth Protection in the Media (Kommission für Jugendmedienschutz, KJM) adopted guidelines clarifying the application of the Interstate Treaty on the Protection of Minors in the Media.[42] Authorities have also developed various resources targeting children online. For example, the EC developed a Better Internet for Kids (BIK+) portal with numerous resources relating to protecting and empowering children and young people online (EC, n.d.[193]; EC, 2022[93]).

Such initiatives are complemented by various best practice principles directed at businesses and awareness initiatives at the global level. The International Consumer Protection Enforcement Network (ICPEN) released best practice principles for online marketing practices directed towards children (ICPEN, 2020[185]) and the CCP's Good Practice Guide on Online Advertising (OECD, 2019[52]) provides tips for businesses on the protection of children or other consumers that may be vulnerable with regard to online advertising. Furthermore, the OECD's global campaigns undertaken each year by the WPCPS intend to increase consumer awareness of a key product safety issue, which may affect children. For example, in 2020, the campaign focused on the safety of children's toys sold online. The 2021 OECD's Guidelines for Digital Service Providers, which support the 2021 OECD Recommendation on Children in the Digital Environment, provide best practice principles for online businesses more broadly, recognising that girls, children belonging to racial, ethnic and religious minorities, children with disabilities, and others belonging to disadvantaged groups may require additional support and protection (OECD, 2021[194]).

In addition, a number of self-regulatory initiatives regarding online marketing directed at children have been implemented in recent years (OECD, 2019[52]). At the international level, general guidance on marketing and advertising by the International Chamber of Commerce includes provisions specific to children (ICC, 2018[195]). In the United Kingdom, the CAP Code includes provisions specific to children (ASA, 2014[196]), and is supported by specific guidance relating to marketing to children, including on marketing to children under 12, age-restricted ads online, advertising in in-game purchases and gambling advertising (CAP, 2017[197]; CAP, 2021[198]; CAP, 2021[199]; CAP, 2022[200]). Moreover, in the United States, the Children's Advertising Review Unit of BBB National Programs, a self-regulatory advertising body, provides guidelines on advertising to children in a range of areas.[43]

Businesses may also offer tools and enact measures to help protect children online. For example, distribution platforms and video game publishers have implemented mechanisms for parents to control the play behaviour of their children, while app marketplaces have also improved their refund practices for unwanted spending (Cerulli-Harms et al., 2020[188]). In addition, businesses may be able to use tools to test the age of the user and/or seek parental authorisation, in order to present more simple information for children and ensure they do not make unauthorised purchases or view inappropriate content for their age (including games and films) (OECD, 2019[2]; OECD, 2018[201]; BMJV, 2021[189]).

Emerging measures and proposals

In several jurisdictions, further regulatory measures are being implemented, particularly in relation to restrictions on targeted advertising and children's personal data. For example, in the European Union, the Digital Services Act (DSA) adopted in 2022 will prohibit online platforms from targeting advertising to a consumer when they can establish with reasonable certainty that the consumer is a minor; require platforms to put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors; and require the terms and conditions of intermediary services directed at minors to be explained in a way that minors can understand. In the United States, in 2022 California's legislature passed the California Age-Appropriate Design Code Act, which once in force will, inter alia, prohibit online businesses from using dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected, to forego privacy protection, or to take actions that would harm the child's well-being.[44]

Legislative proposals are also under consideration in various jurisdictions, particularly as a part of broader reforms to privacy and data protection law. For example, the American Data Privacy and Protection Act (ADPPA), a proposed federal privacy and data protection bill, would prohibit online businesses from targeting advertising to consumers whom the business knows to be under age 17, and would establish a Youth Privacy and Marketing Division at the US FTC. [45] In Canada, the Consumer Privacy Protection Act (CCPPA), proposed federal privacy legislation, would define minors' personal information as sensitive and thus bolster existing protections.[46] Researchers have similarly called for further age-related restrictions on online advertising and influencer marketing (Kennedy, Jones and Williams, 2019[88]; Enke et al., 2021[54]).

There have also been recent proposals in many countries to regulate loot boxes. For example, bills were put forward in 2022 in the Netherlands and Spain that would regulate loot boxes under gambling laws,[47] and in the United States bills to ban loot boxes have been proposed at the federal level[48] and in Hawaii. However, there is not yet consensus among legislators and scholars on which regulatory approach to follow, including whether to use consumer protection or gambling law, and for some jurisdictions there is as yet insufficient evidence of harm from loot boxes to take regulatory action (Leahy, 2022[82]).

Measures targeting elderly consumers online

Similar to children, some jurisdictions define older consumers as vulnerable in the law and/or provide special protections for them (see Table 2). But jurisdictions providing specific regulatory measures targeted at elderly consumers in particular appear less common than they do for children.

Some consumer authorities conduct specific activities aimed to empower and protect elderly consumers from detriment. In Japan, in line with the Consumer Safety Act, some municipalities prepare a "Watch Over List" based on data provided by the Consumer Affairs Agency (CAA). The list is shared with relevant public bodies involved in the "watch over" activities to assist in preventing fraud targeting elderly and cognitively impaired consumers. More broadly, consumer authorities have also developed education and awareness campaigns for elderly consumers relevant for the digital environment. For example, the US FTC has a "Pass it on" initiative to encourage the elderly to share knowledge and have conversations with family and friends to raise awareness about scams and fraud, including online (US FTC, 2021[40]; US FTC, n.d.[202]). In 2022, the United States also passed the Stop Senior Scams Act, which established a "Senior Scams Prevention Advisory Group" at the US FTC to bring together federal agency partners, consumer advocates, and industry representatives to focus on ways to better identify and stop scams that affect older adults.[49] The ACCC also provides online guidance for older people on how to avoid scams, including online dating and romance, investment, and rebate scams (ACCC, n.d.[203]). In Portugal, a national movement called MUDA, promoted by the Portuguese government and several companies, universities and associations, provides various self-learning materials for the elderly relating to the digital environment (MUDA, n.d.[204]).

Business initiatives can also help. In Japan, several telecommunications carriers have since 2012 developed "effortless smart phones", i.e. smart phones with larger font size and equipped with simplified functions, which have been taken up by many elderly consumers.[50]

Measures to address digital access and literacy divides

The 2016 OECD E-commerce Recommendation recommends governments and stakeholders develop education and awareness programmes providing consumers with relevant knowledge and skills to access and use digital technology, taking into account the needs of different groups and factors such as age, income, and literacy. The 2021 OECD Recommendation on Children in the Digital Environment also recommends promoting digital literacy as an essential tool for meeting the needs of children in the digital environment (OECD, 2021[23]), and more and more countries are teaching digital literacy in schools.

Often improving digital skills has been pursued through cross-cutting government initiatives. For example, in Japan, in 2022 the government adopted a Basic Policy for the Vision for a Digital Garden City, which

will promote digitalisation and digital skills through collaboration with municipalities[51]. In Korea, a new legal framework ("Digital Inclusion Law") was being developed at the time of writing to alleviate digital polarisation and empower "safety-vulnerable" groups (see above), with the overarching goal of overcoming digital exclusion and digital divides. Moreover, in Canada, an E-vulnerability Index (EVI) tool was developed in 2022 to measure the extent of digital access and skills in the country and strengthen service delivery and digital policies (Fallahi and Gascon, 2022[205]). The tool sums up, in a single score, the extent to which individuals have: the means to be able to access the Internet and the required technologies; the willingness to use these technologies and the Internet; and the abilities or skills to use these technologies.

Consumer authorities can also play a role in developing digital skills through targeted education and awareness programs (OECD, 2014[21]; OECD, 2019[2]). For example, Japan's Consumer Affairs Agency (CAA) released guidance and tips with information regarding AI and consumer data control (CAA, 2020[206]). Similarly, the consumer protection authority of Mexico (PROFECO) published a handout and video in 2020 to raise awareness among consumers, especially those who lack ICT skills, of typical dark patterns (PROFECO, 2020[207]). Moreover, in the United States the FTC, in conjunction with several government and private sector partners, launched OnGuard Online, an interactive educational website that provides practical tips on online shopping, how to guard against Internet fraud, and protect personal information (US FTC, n.d.[208]). The US FTC also offers free resources such as Net Cetera, which is a guide that offers practical advice about topics such as social networking, privacy, and mobile devices for parents, teachers, and other adults who spend time with kids (US FTC, 2018[209]).

Consumer authorities can also facilitate access to information for consumers who may have difficulties with digital communication. In Colombia, for example, deaf consumers can make a video call to the Superintendence of Industry and Commerce to receive general consumer advice via sign language, and preferential telephone assistance is provided for elderly, minors, victims of armed conflicts, and people with cognitive disabilities.

Finally, a range of policy measures exist to bridge the connectivity divide, including national broadband plans and digital strategies, policies to foster competition, promote investment and ease infrastructure deployment (see OECD (2021[210]) for further details). Various social policies and rural development policies can also contribute to access to Internet services (OECD, 2020[69]).

Measures addressing consumer vulnerability more broadly

A range of measures tackling ongoing and emerging consumer risks online

Existing measures and enforcement activity

In line with the 2016 OECD E-commerce Recommendation, many OECD jurisdictions have prohibitions in consumer law on misleading, deceptive, fraudulent and unfair commercial practices. Examples include the EU UCPD, which includes general prohibitions on practices that are deemed unfair, including misleading actions and omissions and aggressive practices, as well as a range of prohibitions on specific practices; or Section 5 of the US Federal Trade Commission Act (FTC Act), which prohibits unfair or deceptive acts or practices in or affecting commerce. These laws continue to be the main tools providing consumer protection authorities with the authority to take action to protect consumers online. On the basis of such laws, in recent years consumer authorities across a range of jurisdictions have taken action against various deceptive, misleading or unfair data practices (OECD, 2019[191]); misleading online advertising and marketing practices such as subscription traps, misleading pricing, disguised advertising and problematic endorsements (OECD, 2019[52]); and practices relating to misleading, fraudulent or unfair reviews and ratings (OECD, 2019[58]). Where practices harming consumers involve their personal data, privacy and

data protection law enforcement also plays an important role. In many of these areas consumer and data protection authorities have also released business guidance to support their activities.

Many consumer and other regulatory authorities were particularly active during the COVID-19 pandemic. For example:

- In France, authorities issued a decree imposing a ceiling on the retail price of hand sanitisers, which were being sold online at rates much higher than before the pandemic (OECD, 2020[37]). The consumer protection authority, DGCCRF, was charged with enforcement of the ceiling.
- In Italy, the consumer protection authority (AGCM) intervened to close websites selling fake cures or stop search engines pointing to illegal pharmacies (Riefa, 2020[43]).
- In Japan, the CAA enforced temporary regulation for several months in 2020 that prohibited reselling face masks and sanitisers to unspecified persons or a large number of people online through stores or other businesses at prices higher than the acquisition prices[52].
- In the United States, over 2020-2021, the FTC sent more than 80 cease and desist demand letters to remove a large number of false claims and deceptive ads from the marketplace and provide a basis for civil penalties under the COVID-19 Consumer Protection Act (US FTC, 2021[40]).

Enforcement action is essential as vulnerability is also a result of systems that fail to assist consumers (Riefa and Saintier, 2020[211]). However, scholars have raised concerns about whether consumer law enforcement is effectively enforcing consumer rights in some jurisdictions, particularly during the pandemic, in light of factors that may constrain enforcement efforts such as inadequate powers, resources, penalties or remedies (Willis, 2017[212]; Riefa, 2020[43]). Concerns have also been voiced more generally regarding enforcement of data protection law particularly in the European Union (BEUC, 2020[213]).

Recent and emerging measures and proposals

Despite relevant existing laws, in many jurisdictions policy makers and regulators have recognised the need for new measures to address a range of emerging consumer risks in the digital world. In some cases, this involves updates to consumer law. For example, in 2022 the EC began a “fitness check” (an evaluation of a group of related policy interventions) on digital fairness, specifically examining the adequacy of the UCPD, Consumer Rights Directive and Unfair Contract Terms Directive in dealing with issues such as consumer vulnerabilities, dark patterns, personalisation practices, influencer marketing, contract cancellations, subscription service contracts, marketing of virtual items and the addictive use of digital products.[53] In 2022, the ACCC advocated for an economy-wide prohibition on unfair trading practices to be legislated in Australia, in order to better address online scams, harmful apps, fake reviews and dark patterns (ACCC, 2022[214]). Subscription traps and fake and incentivised reviews have been a particular focus in certain jurisdictions. For example, in 2020 and 2021, rules were introduced in Argentina and Germany respectively to require businesses to prominently display a cancellation button to facilitate cancellation of online subscriptions, and further measures were announced by the German government.[54] Various US states recently enacted laws covering auto-renewal clauses in business-to-consumer contracts, complementing existing federal legislation on negative option marketing.[55] In 2023, a bill was introduced in the United Kingdom aiming to ban subscription traps and fake reviews.[56] The European Union similarly introduced rules to address fake reviews and paid rankings in search results in 2019. [57] In the United States, the FTC issued advance notices of proposed rulemaking for rules addressing unfair or deceptive fees (US FTC, 2022[215]), the use of reviews and endorsements (US FTC, 2022[216]) and subscription traps (US FTC, 2023[217]).

Other rules seek to improve consumer protection in non-monetary transactions and in relation to consumer data. For example, in 2019 amendments broadened the scope of EU consumer law to digital goods, content and services regardless of whether the consumer pays a price in money, in line with the 2016 E-commerce Recommendation.[58] Major updates to privacy and data protection law have been proposed in

several jurisdictions. For example, the ADPPA in the United States[59] and CCPPA in Canada[60] would create a comprehensive federal consumer privacy and data protection framework of similar scope and principles to the GDPR, and in Australia, privacy and data protection laws were also in the process of review and update at the time of writing.[61] In 2022, the FTC announced that it was considering rules to combat harmful commercial surveillance and lax data security, and issued an advance notice of and held a public forum regarding proposed rulemaking on the issue (US FTC, 2022[218]).[62]

In the area of product safety, voluntary product safety pledges have been established at international and national levels whereby online marketplaces commit to better protect consumers and go beyond their existing legal obligations (OECD, 2022[49]). Some jurisdictions have sought to adapt product safety legislation to new developments online; for instance, the EU in 2023 adopted a new General Product Safety Regulation (GPSR), which will inter alia update existing rules to address safety risks from online sales, including with clear obligations for online marketplaces.[63]

As noted in the 2014 OECD Recommendation on Consumer Policy Decision-making, consumer protection issues may be addressed across all levels and branches of government (OECD, 2014[21]). In that regard, increasingly jurisdictions are taking a holistic approach to addressing digital consumer and other issues across different policy areas and sectors. For example, the EU DSA introduces a wide range of obligations on online intermediaries and platforms (specific rules are further discussed below) and the EU Digital Markets Act (DMA) adopted in 2022 does so for very large online platforms of systemic importance to the EU internal market.[64] The proposed Online Safety Bill in the United Kingdom would also introduce a range of obligations on online platforms, including measures to address online scams and fraudulent advertising.[65] In recent years several jurisdictions, such as the Netherlands, the United Kingdom and Australia, have established fora for regulators from different policy areas to better co-operate in addressing digital consumer issues.[66] Comprehensive consumer education and awareness initiatives can also play a role: in 2021, the German government committed to ensuring high standards of consumer protection, including through comprehensive consumer education, information in several languages and access to information.[67]

Economy-wide data sharing and portability initiatives in several countries, such as the UK Smart Data initiative and Australia's Consumer Data Right, are currently being implemented with a view to empower consumers to use their data and relevant technology to obtain better deals in key sectors (e.g. energy, finance or communications), particularly those who may be more vulnerable to disengagement (UK BEIS, 2021[219]; Australian Treasury, 2021[220]). In the United Kingdom, following the CMA's investigation into the "loyalty penalty", the UK government and sector regulators introduced or considered further measures to address consumer disengagement in essential consumer markets (e.g. financial services and communications), such as price caps, opt-in subscription renewal or automated switching mechanisms (CMA, 2020[221]).

In recent years novel law reform measures have been proposed aiming to address consumer vulnerability in broad terms, particularly in the digital world, involving placing a form of general duty on businesses to achieve good consumer outcomes. Specifically, Siciliani, Riefa and Gamper (2019[75]) have suggested that a "fairness by design" duty, i.e. a general positive duty to trade fairly, be introduced into consumer law as a complement to existing prohibitions, suggesting that it would also assist in protecting consumers beyond existing protections applying to "average" or "reasonable" consumers and be future-proof to developments in e.g. personalisation. Some commentators suggested that a general principle of "fairness by design" or "non-manipulation by design" be incorporated into EU consumer law as part of the UCPD, to mirror the GDPR's "by design and by default" requirements (Hacker, 2021[131]; BEUC, 2022[175]). A similar example of such a duty was implemented by the UK financial regulator (FCA) as a legal instrument in 2022, requiring firms "to act to deliver good outcomes for retail customers." (FCA, 2022[222]).[68] In a similar vein, Willis (2015[176]; 2017[212]) has advocated for "performance-based" consumer law as a form of "fair marketing by design", whereby businesses would need to *"educate rather than obfuscate, develop product designs that align with consumer expectations rather than defy them, and channel consumers toward products that are*

suitable for the consumers' circumstances". Meeting the performance standards would entail ongoing empirical testing by businesses of consumers' actual comprehension of products and their suitability, which through random sampling may ensure all consumers were accounted for and potentially obviate the need for "average", "reasonable" or "vulnerable" consumer standards (Willis, 2015[176]).

Finally, as mentioned above, algorithmic systems also provide the potential to better protect consumers online, such as AI-based web-crawlers that detect dark patterns, unfair contract terms, fake reviews and ratings or unsafe goods sold on websites (OECD, 2020[69]; Contissa et al., 2018[223]). [69] Though this may also entail risks; in 2022 the US FTC issued a report urging policymakers to exercise caution about relying on artificial intelligence as a policy solution to solve online problems (US FTC, 2022[224]).

Considering that in most jurisdictions dark patterns, exploitative personalisation practices and algorithmic bias and discrimination pose particularly novel policy and enforcement questions, the following sub-sections are dedicated to specific measures to address each of these issues.

Specific measures to address dark commercial patterns

The consumer laws prohibiting misleading, deceptive or unfair practices discussed above as well as data protection laws requiring transactions to be conducted with appropriate levels of transparency or consent also address many dark patterns. Consumer and data protection authorities across OECD jurisdictions have accordingly been taking action against a range of dark patterns (see OECD (2022[3]) for an overview, and US FTC (2022[225]) for recent examples of enforcement action in the United States). Competition law may also be a tool to address a dominant firm's use of dark patterns. But enforcement cases to date predominantly relate to a limited set of dark patterns commonly recognised by regulators, which could point to possible gaps in the law, available evidence, or enforcement capacity. In particular, some dark patterns are not clearly deceptive and hence may not be captured by existing general prohibitions on deceptive commercial practices (such as those termed "confirmshaming" or "nagging") (OECD, 2022[3]).

Various regulatory measures to respond to dark patterns have been proposed or implemented across OECD jurisdictions, in part as a result of uncertainty as to whether existing measures provide sufficient protection to consumers. In the European Union, for example, 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. Some measures seek to prohibit specific kinds of dark patterns; for example, various states in the United States have prohibited the use of dark patterns for obtaining consent for collection and use of personal data, and measures in other countries, as discussed above, were introduced to combat dark patterns that make it hard to cancel or opt out of certain settings or transactions, including subscription traps. Other measures relate to fostering the development of consumer-friendly choice architecture, further empowering regulators to take action against dark patterns and issuing guidance to assist businesses' compliance with relevant existing laws. However, much 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 in light of empirical evidence (OECD, 2022[3]).

Technical tools have also emerged to help address dark patterns and other measures can help raise awareness and educate consumers about them. Various business initiatives and tools may also assist in addressing them, including some existing self- or co-regulatory initiatives. However, while such measures can play an important supporting role, they are insufficient in isolation and should be seen as complementary to robust regulatory and enforcement measures (OECD, 2022[3]).

For further details on measures to address dark patterns, see the CCP's report on the topic (OECD, 2022[3]).

Specific measures to address exploitative personalisation practices

Existing measures

Personalisation practices are not prohibited per se in OECD jurisdictions. Nonetheless, under some circumstances they may contravene existing consumer laws. In particular, where they are combined with ancillary misleading or deceptive practices they may, similar to some dark patterns, contravene prohibitions on misleading or deceptive commercial practices existing in most OECD jurisdictions, such as in the EU UCPD, Articles 6 and 7, or the US FTC Act, Section 5. For example, targeted advertising or differential pricing could potentially be considered misleading if their personalised character is not clarified by, for instance, informing the consumer that some options may not be available to them as a result of the personalisation (e.g. because the consumer is excluded from target categories) (Paterson et al., 2021[115]; Riefa, 2021[226]). Indeed in 2019 EU consumer legislation was amended to explicitly require businesses to inform consumers about the fact that an online price was personalised on the basis of automated decision-making (EC, 2021[163]).[70] Other ancillary misleading or deceptive practices whose use could potentially be grounds to challenge personalisation practices include stating that a personalised offer is the "best" or "discounted" when other consumers are offered better options; falsely stating that a personalised offer will be available for a very limited time (OECD, 2018[104]); or not presenting a (personalised) ad to a consumer that could benefit them (Laux, Wachter and Mittelstadt, 2021[227]).

However, as illustrated in the examples in Section 1, an exploitative personalisation practice may not necessarily involve factual errors or omissions in a representation to a consumer or otherwise deceive them (as is the case for several dark patterns, as discussed above), but instead provision of truthful information at an opportunistic time to exploit a vulnerability (Manwaring, 2018[228]; Chen and Miotto, 2022[229]). In such cases, scholars consider it unlikely that prohibitions on deceptive commercial practices would apply to such practices (Chen and Miotto, 2022[229]; Manwaring, 2018[228]; Greiss, 2021[230]; Calo, 2014[102]). Moreover, disclosing the personalised nature of a practice is unlikely to be sufficient in isolation as a protective measure, including because consumers often do not react strongly to such disclosures (as many empirical studies have shown; see e.g. OECD (2021[231]) and Strycharz et al. (2021[232])) and may not fully grasp the consequences of personalisation.

Nonetheless, in certain circumstances such practices could potentially be challenged under other kinds of principle-based consumer law prohibitions existing in some jurisdictions, of which examples are listed in the table below. Generally such provisions aim to protect consumers from practices that seek to exploit a consumer's disadvantage or weakness.

Table 3. Examples of principle-based consumer law prohibitions other than on deceptive practices that may address exploitative personalisation practices

Jurisdiction	Relevant laws
Australia	Particularly egregious forms of personalisation practices that take advantage of consumers' lack of bargaining power or a position of disadvantage in a manner that is contrary to community values could potentially be considered a form of unconscionable conduct, which is prohibited under the Australian Consumer Law, Section 21 (Paterson et al., 2021[115]; Greiss, 2021[230]; Manwaring, 2018[228]).[71]
Canada	In Ontario, prohibitions on unfair practices that include "unconscionable representations" may impose some limitations on personalised pricing. As stated in the Consumer Protection Act, for the purpose of determining whether a representation is unconscionable, it may be taken into account, among other things, *"that the price grossly exceeds the price at which similar goods or services are readily available to like consumers"* (OECD, 2018[104]).
European Union member states	Prohibitions in the EU UCPD on practices that both materially distort the economic behaviour of the average consumer and are contrary to the requirements of professional diligence (Article 5) or on practices that are aggressive (Articles 8 and 9) could potentially be applied (EC, 2021[163]). The latter may in particular apply when personalisation practices amount to a form of manipulation in which the business exercises "undue influence" over the consumer, particularly where it exploits a specific misfortune or circumstance of such gravity as to impair the consumer's judgement, of which the business is aware (Helberger et al., 2021[111]; Strycharz and Duivenvoorde, 2021[108]; Laux, Wachter and Mittelstadt, 2021[227]; EC, 2021[163]).[72]
Israel	Section 3 of the Consumer Protection Law prohibits businesses from exerting unfair influence on the consumer. This includes taking advantage of any mental, psychological or physical disability of a consumer, of which the business is or ought to be aware (UNCTAD, 2018[181]).
Morocco	Law 31-08 Enacting Consumer Protection Measures, Article 59 provides that abusing a consumer's "weakness or ignorance" ("abus de la faiblesse ou de l'ignorance") may lead to a contract's nullification, consumer refunds and payment of damages (Simpson, 2020[36]).
United States	Personalisation practices that cause substantial injury to consumers that cannot reasonably be avoided (e.g. because they are highly personalised) and are not outweighed by countervailing benefits (e.g. for competition) could potentially be challenged under the FTC Act's Section 5 prohibition on unfair practices (Hirsch, 2020[105]). According to Willis (2020[47]), examples of such practices include in particular those that take advantage of pre-existing false consumer beliefs about facts material to a transaction (e.g. a belief that that consumer is not engaging in a transaction or that their data will not be used in an exploitative manner).

Source: See sources in table

However, some researchers have noted additional challenges to enforcing consumer law prohibitions. First, establishing proof of personalisation practices' deceptive or manipulative character may be difficult, as the characteristics of a personalisation practice presented to the affected consumer(s) may not be similarly observable by a consumer authority or a judge, especially without access to the business' data or knowledge of the consumer's personal vulnerabilities (Milano et al., 2021[233]; Willis, 2020[47]). In addition, where such practices 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[47]). 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 (EC, 2022[95]; Helberger et al., 2021[111]; Willis, 2020[47]).

Beyond consumer law, privacy and data protection law also plays a role. In line with the OECD Privacy Guidelines (OECD, 2013[234]), privacy and data protection regulatory frameworks in most OECD countries require that businesses comply with a range of obligations in relation to the collection of use of personal data, such as disclosing the purposes for which personal data is collected and where applicable obtaining consent for those uses. Hence where personalisation practices rely on data processing that does not satisfy applicable data protection requirements, privacy and data protection authorities may take action against them. However, many commentators assert that even where personalisation practices meet applicable standards of consent, consumers are often unlikely to be able to meaningfully give consent to such practices, for a range of reasons (Hirsch, 2020[105]; Paterson et al., 2021[115]; Strycharz and Duivenvoorde, 2021[108]; Yeung, 2017[145]; Forbrukerrådet, 2021[116]). For instance, as discussed in Section 1, it is difficult for consumers to fully know the ultimate use of their data, even when provided with detailed information disclosures. In addition, sometimes businesses could obtain consent through use of dark patterns, which may not be clearly prohibited (OECD, 2022[3]). Nonetheless, other provisions of privacy

laws may also constrain personalisation practices. For example, the EU GDPR requires that processing of personal data be *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed",* and puts stricter requirements on processing of sensitive personal data (such as on a consumer's health) (Helberger, Borgesius and Reyna, 2017[235]). Similar to some consumer laws, some scholars consider the GDPR's principle of fairness may act as a barrier to data controllers' exploitation of data subjects' vulnerabilities by mitigating excessive unfair imbalances between them (Malgieri and Niklas, 2020[236]). In the Unites States, the California Consumer Privacy Act (CCPA) requires that businesses provide consumers with the option to opt out of the sale and sharing of their personal information, thus reducing the amount of targeted advertising that they receive.

Other solutions could potentially be found in competition law. For example, in circumstances where a dominant firm uses personalisation practices to unfairly gain advantage over rival firms, it may qualify as an abuse of dominance. This could be in the form exclusionary abuse, for instance, where a dominant firm uses personalised pricing to target lower prices to rivals' customers in an attempt to foreclose the market (OECD, 2018[104]). Abuse of dominance could also be in the form of exploitative conduct, in jurisdictions where such conduct is covered by competition law (e.g. the European Union), in situations where personalisation involves use of excessive pricing, unfair contract terms or price discrimination (OECD, 2018[104]; Graef, 2021[237]; Botta and Wiedemann, 2020[238]; ICN, 2021[239]).[73]

However, for many of the above-described potential applications of existing laws, the case law to confirm their applicability is lacking. Accordingly, whether existing regulatory frameworks are adequate to protect consumers from exploitative personalisation practices is in large part yet to be concretely determined.

Emerging measures and proposals

Additional regulatory measures have also been proposed or implemented to address exploitative personalisation practices, particularly targeted advertising, which may reflect concern that existing regulatory frameworks are inadequate. Some relate to providing further information to consumers and the public about personalisation practices. For example, the EU DSA will require that online platforms display meaningful information about the main parameters used to determine the recipient to whom the advertisement is displayed and very large online platforms to, in addition, maintain and provide access to ad repositories, in order for researchers, civil society and authorities to inspect how ads were targeted. Researchers have similarly suggested that online businesses be required to inform consumers when a practice is personalised and the criteria or data on which personalisation is based and set out publicly their approach to targeting and ensuring that it does not result in inappropriate targeting of vulnerabilities. They also propose that very large online platforms be required to make relevant consumer testing data available (Fletcher et al., 2021[77]; Helberger et al., 2021[111]; Strycharz and Duivenvoorde, 2021[108]; Jabłonowska et al., 2018[130]).

Several legislative initiatives involve placing further constraints on consent requirements for targeted advertising. For example, the EU DMA will ban digital platforms with a systemic role in the EU internal market (known as "gatekeepers") from tracking end users outside of their core platform service for the purpose of targeted advertising if effective consent has not been granted. In the United States and Canada, proposed federal privacy bills would introduce, inter alia, constraints on businesses' collection of personal data, transparency obligations on consumer data use, and new consumer rights over their data.[74] Other proposals involve giving consumers more control over whether and what personalisation they are exposed to. These include requiring businesses to respect a consumer's selection of a browser's "Do Not Track" option;[75] requiring a paid version of a service without collection of personal data (Calo, 2014[102]); or giving consumers the choice to not share their data for personalised advertising (CMA, 2020[240]) or to remain invisible from commercial analysis (Hacker, 2021[131]).

Stronger proposals relate to prohibitions on certain forms of personalisation exploiting vulnerabilities. For instance, the EU regulation on artificial intelligence proposed by the EC, the Artificial Intelligence Act (AIA),

would, inter alia, prohibit AI systems that either deploy subliminal techniques or exploit vulnerabilities[76] related to age, physical or mental disability in order to materially distort consumer behaviour such that it causes physical or psychological harm (EC, 2021[241]). In a similar vein, scholars suggest that there be new prohibitions on personalisation practices based on characteristics or circumstances that predict vulnerability, including of a situational nature, as well as on the use of psychographic profiles to exercise emotional or psychological pressure (Fletcher et al., 2021[77]; Helberger et al., 2021[111]; Strycharz and Duivenvoorde, 2021[108]).

Whether measures currently planned will adequately address exploitative personalisation remains to be seen. Some scholars, for example, suggest that measures such as the EU DSA and AIA may need to be complemented with others (Hacker, 2021[131]). In that regard, in 2022 US lawmakers, with the support of several scholars and public interest organisations, introduced the Banning Surveillance Advertising Act (BSAA), a bill that would prohibit targeting advertisements to consumers based on personal information all together (while allowing contextual advertising). Other stakeholders, including regulators (the European Data Protection Supervisor (EDPS, 2021[242])) consumer and other public interest organisations (e.g. Forbrukerrådet (2021[116])) and researchers (e.g. Woodcock (2018[243]) and Rahman and Teachout (2020[244])) have similarly supported such a ban. A total ban would place less reliance on laws that may have gaps for certain kinds of exploitative personalisation practices. But a substantial disadvantage is that the benefits of targeted advertising would also be lost (Strycharz and Duivenvoorde, 2021[108]; Graef, 2021[237]), including the provision of a range of "free" services and content, including social media. One study found, based on a survey of European consumers, that many sites would face serious financial challenges if they depended on subscriptions rather than targeted advertising (IAB Europe, 2020[245]); though other evidence suggests publishers could move from behavioural to contextual advertising without loss of advertising revenue (Forbrukerrådet, 2021[116]).

Finally, educational and technical measures may also address exploitative personalisation practices, such as raising consumers' awareness about them and deploying tools such as browsers that block tracking. Though as with dark patterns, such measures are unlikely to be sufficient in isolation and should complement regulatory and enforcement measures.

Specific measures to address discriminatory and biased algorithms

Existing measures

The 2019 OECD Recommendation on Artificial Intelligence calls on organisations that deploy or operate AI to respect fairness and non-discrimination, inter alia, and implement relevant mechanisms and safeguards (OECD, 2019[246]).

In many jurisdictions it is prohibited to discriminate consumers based on protected characteristics such as gender, race, religion, age, political views, nationality, disability, sexual preferences and marital status. For example, in the European Union, discrimination is prohibited in a number of treaties and constitutions, including Article 14 of the European Convention on Human Rights. Many jurisdictions also have non-discrimination laws applying to the provision of specific services, such as credit, insurance, housing and healthcare.[77] Furthermore, in many jurisdictions laws also prohibit practices that appear neutral but, in practice, disadvantage consumers of a certain protected characteristic; this is often referred to as indirect discrimination (particularly in the European Union) or disparate impact (particularly in the United States). Such laws may in theory be used to challenge algorithms that are indirectly discriminatory (Zuiderveen Borgesius, 2018[247]). For example, in 2020 the US FTC released business guidance on the risks presented by algorithms and AI, which may include unfair or discriminatory outcomes or the perpetuation of existing socioeconomic disparities, and noted how such outcomes may fall foul of US anti-discrimination laws such as those relating to consumer credit (US FTC, 2020[248]).

Indeed a few concrete cases illustrate the role for non-discrimination law. For instance, in the United States in recent years a range of government and public interest bodies have brought cases against a social media platform for discrimination resulting from its advertising algorithms (Zang, 2021[153]), including the US Department of Justice in relation to discriminatory housing advertisements (US DOJ, 2022[249]). Partly in response to regulatory scrutiny, major online platforms have taken measures themselves to mitigate discriminatory outcomes in relation to advertising.[78]

However, some researchers consider that non-discrimination law leaves important gaps (Zuiderveen Borgesius, 2020[250]; Wachter, 2019[251]). For instance, it may have gaps in relation to discriminatory outcomes for certain protected characteristics,[79] as well as for outcomes that are unrelated to a defined protected characteristic (e.g. browser type or low income) but that may still be considered unfair (for instance if they reinforce social inequalities) (Zuiderveen Borgesius, 2018[247]). Laws governing indirect discrimination or disparate impact may also be difficult to apply in practice.[80] Furthermore, evidence of discrimination may be lacking as algorithms often operate opaquely and consumers may often be unaware of it themselves.

Nonetheless, privacy and data protection law may offer another avenue to challenge algorithmic bias. For example, transparency and consent obligations would need to be satisfied under data protection law for processing of personal data by algorithms (Zuiderveen Borgesius, 2018[247]). In addition, the EU GDPR, under certain circumstances, prohibits the processing of personal data relating to a range of protected characteristics and offers various protections against decisions based on automated processing (EDRi, 2021[252]). But data protection law protections may also be insufficient at times, including because some algorithms do not process personal data (Zuiderveen Borgesius, 2018[247]; Wachter, 2019[251]).

In some cases, algorithmic discrimination might be challenged under consumer law, e.g. when it also involves deception or manipulation similar to exploitative personalisation practices (see above). Though this remains relatively unexplored compared to non-discrimination and data protection law (Zuiderveen Borgesius, 2018[247]; CMA, 2021[147]). In 2021 the US FTC indicated it would explore how it could apply the prohibition on unfair trading practices in US law (see above) to target discriminatory practices (US FTC, 2021[253]), suggesting that the sale or use of racially biased algorithms, for example, could fall within its scope; such an application is also supported by researchers (Hirsch, 2020[105])[81] and existing cases.[82] Similarly, under certain circumstances discriminatory algorithms could meet the bar of an unfair trading practice in US financial consumer protection law (CFPB, 2022[254]).[83] The CMA indicated consumer law could also potentially be used to protect groups of consumers with vulnerabilities that have not been firmly established as protected characteristics, thus potentially making up for gaps in non-discrimination law described above (CMA, 2021[147]).

Overall, however, as with exploitative personalisation practices, sufficient case law involving algorithmic consumer discrimination to test the robustness of non-discrimination, privacy and data protection and consumer laws is lacking. Consumer authorities and other commentators have furthermore encouraged businesses to be transparent to consumers on their use of algorithms, to self-audit decision outcomes for bias and to adopt other principles (Zang, 2021[153]; Lee, Resnick and Barton, 2019[156]; US FTC, 2020[248]; ACM, 2020[169]). But many guidelines are non-binding and lack an enforcement mechanism, suggesting a potential role for additional regulation (CMA, 2021[147]).

Emerging measures and proposals

Generally speaking, approaches proposed to mitigate discrimination in AI systems range from awareness building; organisational diversity policies and practices; standards; technical solutions to detect and correct algorithmic bias; and self-regulatory or regulatory approaches (OECD, 2019[150]).

Some legislative measures or proposals have sought to more explicitly ban discrimination in advertising or in the use of personal data. In particular, in the European Union, the DSA will explicitly ban targeted advertising on online platforms based on special categories of sensitive data as defined by the GDPR,

which include ethnicity, political views or sexual orientation. In the United States, the BSAA would prohibit targeted advertising based on membership of a protected class, and the ADPPA would prohibit most businesses from using data in a way that discriminates on the basis of protected characteristics. Researchers similarly propose additional regulation to prohibit platforms from discriminating against consumers based on protected characteristics or any group identified as vulnerable to particular sales practices or services (Fletcher et al., 2021[77]).

Legislative initiatives governing AI proposed in various jurisdictions would require businesses to conduct impact assessments to ensure algorithms are not biased. For instance, the EU AIA would require providers of "high-risk" AI systems, which would include those used in certain private services deemed essential such as credit scoring, to conduct ex ante conformity assessments and post-market monitoring plans of such systems and ensure high quality data sets to minimise discriminatory outcomes.[84] In Canada, the proposed Artificial Intelligence and Data Act would impose an obligation on persons responsible for high-impact AI systems to identify, assess, and mitigate risks of harm or biased output.[85] In the United States, the proposed Algorithmic Accountability Act and the ADPPA would similarly require businesses and large data holders respectively to conduct impact assessments of their automated decision systems or algorithms to test for bias, among other requirements.[86] Researchers have similarly supported a requirement for businesses to develop "bias impact statements" (Lee, Resnick and Barton, 2019[156]).

Additional measures proposed include improving the funding and investigatory powers of regulatory bodies, such as consumer protection and data protection authorities, equality bodies and human rights monitoring bodies (EDRi, 2021[252]; Zuiderveen Borgesius, 2018[247]); updating existing non-discrimination laws for the digital age, e.g. through clarifications on application to algorithms (Lee, Resnick and Barton, 2019[156]); enacting further sector-specific laws, in consideration of the different risks and principles applying in different sectors (Zuiderveen Borgesius, 2018[247]); and establishing greater procedural "due process" protections, including by disclosing how algorithms arrived at an output and providing consumers and regulators access to an audit trail (Hirsch, 2020[105]; CMA, 2021[147]).

3 Strengthening the evidence base on consumer vulnerability in the digital age

Gaps in evidence on consumer vulnerability

Consumer surveys, complaints collected by consumer authorities and organisations as well as behavioural experiments often include data on consumers' socio-demographic characteristics. But as discussed in Section 1, a conceptualisation of consumer vulnerability in the digital age as "systemic" or "universal" largely reflects a state-based approach, whereby vulnerability results not necessarily or only from personal characteristics, but from a combination and interaction of factors both internal and external to the consumer, of temporary or permanent in duration, such that all consumers could be vulnerable in certain circumstances. Following a meta-review of articles published between 2010 and 2019 examining consumers experiencing vulnerability, Riedel et al. (2021[255]) concluded that most research has focused on specific individual characteristics driving vulnerability, such as age or socioeconomic status. Much less research has been conducted on external conditions (e.g. market practices), individual states (e.g. emotions and physiological states) and certain other personal attributes or circumstances (e.g. gender or geographical remoteness). Research examining vulnerability due to external conditions has also decreased over time, while the focus on internal characteristics has increased. Strycharz and Duivenvoorde (2021[108]) also note that empirical research that operationalises contextual and external types of vulnerabilities and their role in consumers' online interactions with businesses is still scarce. These findings underline the need for more targeted research on consumer vulnerability online in such areas to better target policy measures.[87]

Using traditional empirical methods to expand the evidence base

The 2016 EC vulnerability study sought to operationalise a state-based conceptualisation of vulnerability for empirical analysis, by translating its key dimensions identified in the literature into measurable indicators of vulnerability. Such indicators were then mapped to key questions/variables in a consumer survey and behavioural experiments conducted in several countries and multiple sectors, as shown in the table below.

Table 4. Example of operationalisation of dimensions of vulnerability for empirical analysis

Dimension	Indicators	Questions/variables
1.Heightened risk of negative outcomes or impacts on well-being	1. Unassertive when experienced a problem buying or using goods or services	Did not take action when experienced a problem when buying or using goods or services in last 12 months
	2. Overpaid for services	Paid more for services in last 12 months due to being unable to use a certain payment method
2. Having characteristics that limit ability to maximise well-being	3. Perception of own vulnerability due to personal characteristics	Feels vulnerable because of health problems, financial circumstances, employment situation, age, belonging to a minority group, personal issues, other reasons
3. Having difficulty in obtaining or assimilating information	4. Does not feel informed	How informed feels about prices etc. when buying goods and services
	5. Gets information from few sources	Where gets information to compare deals
	6. Does not compare deals due to information-related factors	Whether compares deals How difficult finds it to compare deals Why finds it difficult to compare deals Why never compares deals
	7. Has not recently switched due to being unsure about where to get information	Whether has switched in last 5 years Why has never switched
4. Inability or failure to buy, choose or access suitable products	8. Does not compare deals due to a) personal, b) market-related and c) access-related factors	Whether compares deals How difficult finds it to compare deals Why finds it difficult to compare deals Why never compares deals
	9. Has not recently switched due to a) personal factors, b) market-related factors, c) access-related factors, d) termination costs and e) bundling of offers	Whether has switched in last 5 years Why has never switched Has not switched in last 12 months due to termination costs or bundling
	10. Excluded from ecommerce	Did not make a purchase online in last 12 months due to difficulty of process or not having payment card
	11. Declined a loan	Whether has tried but failed to obtain a loan in the last 5 years
5. Higher susceptibility to marketing practices	12. Perception of own vulnerability due to marketing practices	Feels vulnerable because offers, terms or conditions are too complex

Source: EC (2016[25]).

The study specified that whether it is appropriate to examine particular or all dimensions of vulnerability should be decided based on initial scoping work, which may take into account gaps in the existing evidence and policy objectives. For example, where a specific marketing practice is of concern, “high susceptibility to marketing practices” could be the focal point; where a sector is widely recognised for information problems, “having difficulty in obtaining or assimilating information” could be in focus.

Implicit in such dimensions is the range of factors the study identified linked to vulnerability going beyond personal and demographic characteristics, such as behavioural drivers, market-related drivers, access drivers and situational drivers, as shown below.

Table 5. Example of operationalisation of drivers of vulnerability for empirical analysis

Driver of vulnerability	How operationalised in 2016 EC vulnerability study
Personal and demographic characteristics	• Age • Gender • Population density of the respondent's region of residence • Household size • Education level • Whether the respondent's mother tongue is different from the official language(s) spoken in their country of residence
Behavioural drivers of vulnerability	• Trust in others • Credulity • Willingness to take risks • Impulsiveness • Tests of computational ability • Knowledge of terms relating to the energy and online sectors and ability to identify the best interest rate for a savings account
Market-related drivers of vulnerability	• Respondent's knowledge of their contract • Being unable to read the terms and conditions of a contract because of small print • Frequency with which the respondent compares deals • Whether the respondent read the last bill or communication from their provider (in each sector) • How easy the respondent found it to read the last bill or communication from their provider (in each sector)
Access drivers of vulnerability	• Frequency of Internet use for the purposes of online search, comparison of prices, online banking, online purchases, online selling, social media, and email • The number of purposes (listed above) the respondent uses the Internet for at least once a month
Situational drivers of vulnerability	• Occupational status • Whether the respondent finds it easy to 'make ends meet' (a proxy for the state of their finances) • Personal situation (married, remarried, not married living with a partner, single, divorced or separated, widowed or other) • Number of dependent children • Whether the respondent is a single parent • Measures describing the respondent's social circles (having friends who buy on-line, buy on credit, or can't make ends meet

Source: EC (2016[25]).

The 2016 EC vulnerability study provides an initial illustration of how traditional empirical methods can be applied to assess dimensions and drivers of consumer vulnerability that go beyond personal and demographic characteristics (EC, 2016[25]). Similarly, the 2021 CCP survey added to the empirical literature of a broader understanding of consumer vulnerability by testing consumer outcomes in e-commerce in terms of a range of drivers of vulnerability. These included questions regarding personal and demographic characteristics (age, gender, population density of respondent's region of residence, education level), behavioural drivers (trust, willingness to take steps to resolve a problem, extent to which consumer reads information online), access drivers (frequency of use of Internet for e-commerce), situational drivers (occupational status, income, ability to make ends meet), as well as a range of questions regarding the nature, incidence and magnitude of different problematic practices experienced (OECD, 2022[4]). An earlier EC survey on measuring consumer detriment in six markets similarly collected data on several drivers of vulnerability (EC, 2017[62]).

Hence well-designed quantitative surveys can usefully contribute to a more comprehensive understanding of consumer vulnerability in the digital age through statistically robust measurements of indicators of different key drivers of vulnerability. Nonetheless, in some cases they may suffer from specific shortcomings:

- Issues relating to some drivers of vulnerability are less likely to be captured by quantitative surveys. For example:

  - Some consumer groups are unlikely to be captured in quantitative surveys however large the size (EC, 2017[62]), e.g. consumers with digital access or literacy problems or visual impairment, particularly when the survey is online and such consumers are unlikely to be included in recruitment panels (EC, 2016[25]).
  - Detriment resulting from market practices that are hidden to consumers, e.g. algorithmic bias or misuse of personal data, will not be captured in responses.
- Some consumer groups may have developed a systematic tendency for lower expectations of outcomes (e.g. minorities that have grown to expect some level of discrimination), such that survey-based measurements of detriment based on problems for which consumers had a "legitimate cause for complaint" (e.g. OECD (2022[4]) and EC (2017[62])) may understate their negative outcomes (EC, 2007[256]).
- Qualitative details on vulnerability, such as the reasons for which some consumers disproportionately suffer detriment, are often impractical to collect in a large quantitative survey (EC, 2017[62]).

Complaint data can often suffer from the same pitfalls in terms of representativeness (e.g. lack of complaints for hidden detriment or a lower propensity to complain for certain consumer groups).

Behavioural experiments are another key way to explore consumer vulnerability in the digital environment and may address some of these shortcomings. They can be particularly useful to simulate market situations, the impact of certain online commercial practices and the effectiveness of remedies (for an overview of experiments testing online disclosures and dark patterns see OECD (2022[79]) and OECD (2022[3]) respectively). Well-designed experiments can also more closely explore vulnerability beyond personal and demographic characteristics, such as situational drivers (e.g. time pressure (EC, 2022[95])) or behavioural drivers (e.g. willingness to take risks (EC, 2016[25])). Experiments that approximate real-life settings may generate data on the real impacts of market practices on consumers, which may not be reported in the same way in surveys. Field experiments, involving real-world testing environments, may also capture data on consumers who would otherwise not be recruited in online experiments. Follow-up questions can also be asked to respondents to explore aspects from a qualitative perspective, including why respondents made certain decisions (EC, 2016[25]). Questions prior to the experiment, e.g. regarding personality, can also be asked to personalise the experiment and test vulnerabilities at a more granular level (EC, 2022[95]).

Another possible alternative is to identify relevant consumer groups for targeted interviews or focus groups with such consumers, potentially combined with interviews with experts relevant for such consumer groups (EC, 2017[62]). In recent years qualitative end-user experience studies focusing on dark patterns, for example, have begun to emerge (Maier and Harr, 2020[257]; Gray et al., 2021[258]). However, interviews and focus groups are generally conducted at a small scale and hence may lack the statistical robustness of large quantitative surveys and online experiments. As a result, a mix of multiple methods is often appropriate[88] and may also extend coverage of different drivers of vulnerability. Combining evidence with transaction data may also assist; for example, the CMA considered the best way to collect evidence on the "loyalty penalty" was through matching price and other transaction data from suppliers across a range of markets with a recurring survey containing comprehensive information about respondents' characteristics (such as income, age, mental health and any physical disability/health conditions) (CMA, 2019[27]).

Outlook: towards novel methods

The above discussion illustrates how traditional empirical methods, such as consumer surveys, behavioural experiments, complaints analysis, focus groups and interviews, when well-designed, can capture data on a number of factors driving consumer vulnerability online. Still, vulnerabilities that are

temporal, contextual or idiosyncratic may not be fully captured by such methods, including because the marketing practice may not be observable to the consumer and the consumer may not be aware of their own vulnerabilities. Experimenting with the exploitation of personal vulnerabilities can also raise ethical concerns (EC, 2022[95]). Hence in some cases novel methods may need to be explored. For example, neurophysiological experiments can be conducted to test vulnerabilities relating to specific cognitive burdens and difficulties (see e.g. EC (2022[95])). According to Strycharz and Duivenvoorde (2021[108]), the link between personalised marketing and consumer vulnerabilities could be analysed through "digital trace data" collected through tracking consumer behaviour and their exposure to certain personalisation practices (Bol et al., 2020[120]), or through the use of publicly accessible databases documenting advertisements on different platforms (Leerssen et al., 2019[259]). More broadly, to the extent online businesses make their own experimental testing and the inputs and outputs of algorithms available to researchers and regulators (as proposed under certain measures discussed above), this would also allow for greater empirical analysis of dark patterns, exploitative personalisation practices and algorithmic bias and discrimination (as also discussed in the CCP's roundtable on consumer vulnerability in the digital age (Annex A)).

The CCP will continue to develop evidence on consumer vulnerability in its research agenda, working with other relevant international fora and stakeholders. This includes, in particular, empirical work aimed to assess consumer attitudes and behaviour towards dark patterns, sustainable consumption, and online product safety to be undertaken over the course of 2023-2024.

Annex A. Extract of summary record of roundtable discussion on consumer vulnerability at the CCP's 100th Session[1]

A roundtable was held to explore ongoing and emerging consumer issues associated with the changing nature and extent of consumer vulnerability in the digital age. The discussion was informed by short presentations from speakers from academia, consumer authorities and civil society, and was moderated by Mr. Dries Cuijpers, Senior Enforcement Official from the Netherlands Authority for Consumers & Markets.

The roundtable began with a presentation from **Prof. Hans-W. Micklitz**, Professor for Economic Law, Robert Schuman Centre for Advanced Studies at the European University Institute and Finland Distinguished Professor, University of Helsinki. Mr. Micklitz argued that the traditional understanding of "vulnerable consumer" relating to specific consumer groups, adopted for example by the EU UCPD, should be revised. He highlighted in particular that in digital markets, where all consumers have a persuasion profile, the vulnerable consumer is no longer the exception, nor is the average consumer the rule – instead every consumer could be vulnerable to certain practices at certain times. Mr. Micklitz pointed to a recent study developed for the BEUC (European Consumer Organisation) that he co-authored, which advances the concept of digital vulnerability, understood as a "*universal state of defencelessness and susceptibility to the exploitation of power imbalances that are the result of the increasing automation of commerce, 'datafied' consumer-seller relations and the very architecture of digital marketplaces"* (Helberger et al., 2021[111]). He argued that digital vulnerability is both architectural, due to data-driven choice architectures employed by online businesses, and relational, due to the lasting relationships that online businesses build with consumers through ongoing personalisation. He suggested that a new understanding of "digital vulnerability" may need to be anchored in the law, accompanied by a reversal of the burden of proof in business-to-consumer transactions and prohibitions of certain online commercial practices causing consumer harm.

Mr. Gunstein Instefjord, head of the consumer advocacy unit at the Norwegian Consumer Council (Forbrukerrådet), then presented some of the Council's work on consumer vulnerability, arguing that consumers cannot be expected to be experts and make rational decisions in all their transactions, particularly those they do not understand. He noted that as a result of a range of factors – including consumer profiling, use of manipulative dark commercial patterns, increasing personalisation and individualisation of digital services, and the dominant positions of digital platforms – all consumers could potentially be considered vulnerable online.

Ms. Ana Catarina Fonseca, Director-General of the Consumer Directorate-General of Portugal, presenting as President of FIAGC (Iberoamerican forum of Consumer Protection Agencies), confirmed that all consumers can experience situations of vulnerability. She noted that the pandemic had deepened existing situations of vulnerability and rendered vulnerable some consumers who had never had any experience of vulnerability before. She argued that online transactions raise special challenges owing to

[1] The CCP's 100th Session summary record is contained in document DSTI/CP/M(2021)1.

the vast range of goods and services and dynamic nature of commercial practices. She then introduced the results of a survey of FIAGC members aimed at understanding how they address the needs of vulnerable consumers, which found that the effects of the pandemic, combined with socioeconomic conditions and personal characteristics related to age and gender, had resulted in increased levels of vulnerability in many countries. Financial vulnerability/indebtedness appeared to be important points of concerns for countries. Ms. Fonseca further noted that Spain's and Argentina's existing legislation included a legal definition of vulnerable consumer, and that several FIAGC members had developed specific education programs targeting certain consumer groups (including children and young people, elderly, migrants and women) as well as measures to provide support to over-indebted consumers.

Ms. Helena Leurent, Director General, Consumers International (CI) shared reflections on consumer vulnerability drawing on work in this area by CI and its members. She first stated that during the COVID-19 pandemic, an increasing number of consumers had engaged in digital markets, many of whom were first-time users. She highlighted that the notion of consumer vulnerability was evolving particularly as a result of data-driven and personalised transactions. She pointed to the results of a survey of CI members in 2020, which showed that only 50% of countries surveyed had a law relating to "vulnerable consumers", despite a substantial rise in online scams and the fact that even experienced consumers were facing issues with online transactions. Finally, she emphasised the importance of sharing international experiences in this area.

Ms. Yasuko Iwai, Deputy Director of International Affairs Office, Consumer Affairs Agency (CAA) of Japan, introduced the agency's work on consumer vulnerability focusing on AI and data control. She first noted that the notions of "average" or "reasonable" consumer were not explicitly included in Japan's consumer laws. She also presented the results of CAA's "Study on Response to Digitalization", which considered issues around inappropriate use of digital technology, lack of ICT knowledge and other issues such as rapid increase of illegal or harmful content online. Ms Iwai stated the importance of effective consumer education and awareness raising activities. She also introduced two education materials recently published by the CAA aimed to address vulnerability online, a Guidebook for Digital Platform Transaction Users, and a handbook on AI Utilization.

Mr. Andrew Hadley, Assistant Director, Policy, Advocacy and International, Office of the General Counsel, United Kingdom Competition and Markets Authority (CMA), focused his intervention on changing consumer vulnerabilities, noting that consumer authorities should move away from an approach focusing solely on particular types of vulnerable consumer groups in light of emerging digital practices. He pointed to the CMA's distinction between vulnerability relating to personal characteristics and situational or market-specific vulnerability. He emphasised the role of "hot states" in leading consumers to make sub-optimal decisions in the online environment and the challenge of balancing the need to protect online consumers with businesses' need to remain competitive in the market. To guard against algorithmic discrimination, Mr. Hadley suggested that consumer authorities focus more on regulating the outcomes of algorithms rather than the inputs. He also mentioned the UK's Smart Data Review, a project involving improving outcomes for vulnerable consumers through better use of their consumer data in certain key sectors (e.g. usage data in energy, finance or communications) and technology, as well as the CMA's recent work on consumer vulnerability.

Mr. Pierre Chalançon, Chair of Business at OECD's (BIAC) Consumer Policy Committee, highlighted the importance of providing a holistic response to emerging risks in the digital age, which should address consumer vulnerabilities resulting from exposure to illicit and unsafe goods online. Enhancing consumer education and awareness, strengthening public and private partnerships, and adjusting existing frameworks to the digital environment were all mentioned as key priorities. Finally, he presented BIAC's recent statement on "Protecting Consumers on Online Marketplaces".

In the discussion that followed, Ms. Juliana Domingues, National Consumer Secretary in Brazil, indicated that consumer vulnerability affecting low-income consumers, the elderly, and people with disabilities, was

an important policy focus in Brazil. She also noted how a series of cases of unauthorised sales of vaccines on websites linked to possible scams that emerged during the pandemic. Ms. Stacy Feuer, Assistant Director at the United States Federal Trade Commission (US FTC), noted that the FTC would be looking more closely at consumer and privacy law violations that affect vulnerable consumers disproportionately, particularly in the digital environment, including biased and discriminatory algorithms. She also pointed to business guidance that the FTC released in April 2020 covering discriminatory risks of AI and underscored the need to consider both inputs and outcomes of algorithms to assess possible impacts on vulnerable consumers. She further highlighted a workshop on dark patterns to be held by the FTC on 29 April 2021.

The following points summarise the discussion:

- Consumer vulnerability is taking on new forms in the digital era as a result of a range of factors, including different consumer behaviour in the online world, discrimination through use of AI and algorithms, increased data collection, consumer profiling and personalisation, and potentially harmful digital choice architectures.
- Whilst the definition of vulnerable consumers in the OECD's 2014 Recommendation on Consumer Policy Decision Making is still broadly relevant in the digital age and provides an appropriate frame for addressing vulnerability, there may be a need to expand it on particular aspects, for example by noting specifically that transactions of a personalised nature may drive greater vulnerability.
- Likewise, in this context, it may be necessary to rethink how to understand and apply legal standards of "average" or "reasonable" consumer as well as existing policy or legal definitions of "vulnerable" consumers.
- Despite growing awareness of increased consumer vulnerability, data on the harm suffered by vulnerable consumers seems to be lacking, and greater efforts are needed to strengthen the evidence base. Data could for example be gathered on any bias in the output data of algorithms or on higher prices charged to vulnerable consumers.
- Building on such data, existing regulatory and enforcement responses may need to be revisited to address consumer vulnerability in the digital age more effectively.

References

ACCC (2022), *Digital Platform Services Inquiry. Discussion Paper for Interim Report No.5: Updating competition and consumer law for digital platform services*. [214]

ACCC (2021), *Consumer vulnerability: A business guide to the Australian Consumer Law*. [28]

ACCC (2021), *Press release: "Culturally and linguistically diverse community lose $22 million to scams in 2020, reports from Indigenous Australians up by 25 per cent"*, https://www.scamwatch.gov.au/news-alerts/culturally-and-linguistically-diverse-community-lose-22-million-to-scams-in-2020-reports-from-indigenous-australians-up-by-25-per-cent. [60]

ACCC (2019), *Digital Platforms Inquiry*. [80]

ACCC (n.d.), *Advice for older Australians*, https://www.scamwatch.gov.au/get-help/advice-for-older-australians. [203]

ACCC (n.d), *Online shopping scams*, https://www.scamwatch.gov.au/types-of-scams/buying-or-selling/online-shopping-scams. [59]

ACCC (n.d.), *Scam statistics*, https://www.scamwatch.gov.au/scam-statistics. [39]

ACM (2021), *Sponsored ranking: An exploration of its effects on consumer welfare*. [143]

ACM (2020), *Guidelines on the protection of the online consumer*. [169]

Albertson Fineman, M. (2008), "The Vulnerable Subject: Anchoring Equality in the Human Condition", *Yale Journal of Law and Feminism*, Vol. 20, pp. 1-24, http://ssrn.com/abstract=1131407. [12]

Ali, M. et al. (2019), "Discrimination through Optimization", *Proceedings of the ACM on Human-Computer Interaction*, Vol. 3/CSCW, pp. 1-30, https://doi.org/10.1145/3359301. [155]

Andreasen, A. (1975), *The Disadvantaged Consumer*, Free Press. [265]

ASA (2014), *The CAP Code*. [196]

ASIC (2019), *ASIC Corporate Plan 2019-23*. [31]

Australian Treasury (2021), *Government Response to the Inquiry into Future Directions for the Consumer Data Right*. [220]

Baker, S., J. Gentry and T. Rittenburg (2005), "Building understanding of the domain of consumer vulnerability", *Journal of Macromarketing*, Vol. 25/2, pp. 128-139, [11]

https://doi.org/10.1177/0276146705280622.

Balkin, J. and J. Zittrain (2016), *A Grand Bargain to Make Tech Companies Trustworthy*. [264]

Bell, B. and D. Fitton (2021), *Dark Patterns in Mobile Games: A Source of Online Risk for Youths?*. [100]

Berg, L. (2015), "Consumer vulnerability: are older people more vulnerable as consumers than others?", *International Journal of Consumer Studies*, Vol. 39, pp. 284-293, https://doi.org/10.1111/ijcs.12182. [64]

BEUC (2022), *"DARK PATTERNS" AND THE EU CONSUMER LAW ACQUIS Recommendations for better enforcement and reform*. [175]

BEUC (2020), *THE LONG AND WINDING ROAD: Two years of the GDPR: A cross-border data protection enforcement case from a consumer perspective*. [213]

BMJV (2021), *The second amendment of the Youth Protection Act*, https://www.bmfsfj.de/bmfsfj/service/gesetze/zweites-gesetz-zur-aenderung-des-jugendschutzgesetzes-147956. [189]

Boerman, S., S. Kruikemeier and F. Zuiderveen Borgesius (2017), "Online Behavioral Advertising: A Literature Review and Research Agenda", *Journal of Advertising*, Vol. 46/3, pp. 363-376, https://doi.org/10.1080/00913367.2017.1339368. [114]

Bol, N. et al. (2020), "Vulnerability in a tracked society: Combining tracking and survey data to understand who gets targeted with what content", *New Media & Society*, Vol. 22/11, pp. 1996-2017, https://doi.org/10.1177/1461444820924631. [120]

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*, Association for Computing Machinery, Inc, https://doi.org/10.1145/3461778.3462086. [96]

Botta, M. and K. Wiedemann (2020), "To discriminate or not to discriminate? Personalised pricing in online markets as exploitative abuse of dominance", *European Journal of Law and Economics*, Vol. 50/3, pp. 381-404, https://doi.org/10.1007/s10657-019-09636-3. [238]

Brown, K. (2011), "'Vulnerability': Handle with Care", *Ethics and Social Welfare*, Vol. 5/3, pp. 313-321, https://doi.org/10.1080/17496535.2011.597165. [15]

CAA (2021), *Consumer hotline for Covid-19 vaccination scams*, https://www.caa.go.jp/policies/policy/consumer_policy/information/notice/efforts_001.html#vaccine. [42]

CAA (2020), *Guidance for consumers – How to utilise AI in the digital age*. [206]

Calo, R. (2021), *Comments at US FTC workshop "Bringing Dark Patterns to Light"*, https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf. [129]

Calo, R. (2014), "Digital market manipulation", *George Washington Law Review*, Vol. 82/4, pp. 995-1051, https://doi.org/10.2139/ssrn.2309703. [102]

Calo, R. and A. Rosenblat (2017), "The taking economy: Uber, information, and power", *Columbia Law Review*, Vol. 117/6, pp. 1623-1690, https://doi.org/10.2139/ssrn.2929643. [112]

CAO (2020), *National survey on information communications equipment*, https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd111430.html. [160]

CAP (2022), *Gambling and lotteries advertising: protecting under-18s*. [200]

CAP (2021), *Age-restricted ads online*. [198]

CAP (2021), *Guidance on advertising in-game purchases*. [199]

CAP (2018), *Vulnerable people: How CAP and BCAP protect vulnerable people*. [183]

CAP (2017), *Recognition of advertising: online marketing to children under 12*. [197]

Carrascosa, J. et al. (2014), "I Always Feel Like Somebody's Watching Me. Measuring Online Behavioural Advertising", *Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies, CoNEXT 2015*, https://doi.org/10.1145/2716281.2836098. [121]

Cartwright, P. (2014), "Understanding and Protecting Vulnerable Financial Consumers", *Journal of Consumer Policy*, Vol. 38/2, pp. 119-138, https://doi.org/10.1007/s10603-014-9278-9. [17]

Cerulli-Harms, A. et al. (2020), *Loot boxes in online games and their effect on consumers, in particular young consumers*. [188]

CFPB (2022), *UDAAP Manual V.3 (March 2022)*. [254]

Christl, W. (2017), *HOW COMPANIES USE PERSONAL DATA AGAINST PEOPLE. Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information*. [106]

CI (2021), *Public utilities & vulnerable consumers*. [179]

CI and Mozilla (2022), *A Consumer Investigation into Personalised Pricing*. [136]

CMA (2022), *Evidence review of Online Choice Architecture and consumer and competition harm*. [107]

CMA (2021), *Algorithms: How they can reduce competition and harm consumers*, https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers. [147]

CMA (2020), *Loyalty penalty update - progress two years on from the CMA's super-complaint investigation*. [221]

CMA (2020), *Online platforms and digital advertising - Market study final report*. [240]

CMA (2020), *Protecting consumers during the coronavirus (COVID-19) pandemic: update on the work of the CMA's Taskforce*. [41]

CMA (2019), *Consumer vulnerability: challenges and potential solutions*, https://www.gov.uk/government/publications/consumer-vulnerability-challenges-and-potential-solutions. [27]

CMA (2018), *Pricing algorithms. Economic working paper on the use of algorithms to facilitate collusion and personalised pricing*. [134]

CMA (2017), *Online search: Consumer and firm behaviour - A review of the existing literature*. [142]

CNIL (2020), *Les comportements digitaux des enfants. Regards croisés parents et enfants.*, https://www.cnil.fr/sites/default/files/atoms/files/sondage_ifop_-_comportements_digitaux_des_enfants_-_fevrier_2020.pdf. [90]

Cohen, J. (2019), *Bringing Down the Average: The Case for a "Less Sophisticated" Reasonableness Standard in US and EU Consumer Law*, https://lawecommons.luc.edu/lclr/vol32/iss1/2. [170]

Cole, A. (2016), "All of Us Are Vulnerable, But Some Are More Vulnerable than Others: The Political Ambiguity of Vulnerability Studies, an Ambivalent Critique", *Critical Horizons*, Vol. 17/2, pp. 260-277, https://doi.org/10.1080/14409917.2016.1153896. [14]

Commuri, S. and A. Ekici (2008), "An Enlargement of the Notion of Consumer Vulnerability", *Journal of Macromarketing*, Vol. 28/2, pp. 183-186, https://doi.org/10.1177/0276146708316049. [9]

Contissa, G. et al. (2018), "Towards Consumer-Empowering Artificial Intelligence", *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence*, https://doi.org/10.24963/ijcai.2018/714. [223]

Corones, S. (2014), *Australian Competition and Consumer Commission V TPG Internet Pty Ltd; Forrest v Australian Securities and Investments Commission. Misleading conduct arising from public statements: Establishing the knowledge base of the target audience*. [167]

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. [165]

CPRC (2022), *Duped by Design. Manipulative online design: Dark patterns in Australia*. [97]

CPRC (2020), *Exploring regulatory approaches to consumer vulnerability. A report for the Australian Energy Regulator*. [158]

Datta, A. et al. (2018), "Discrimination in Online Advertising A Multidisciplinary Inquiry", *Proceedings of Machine Learning Research*, Vol. 81, pp. 1-15. [263]

Datta, A., M. Tschantz and A. Datta (2015), "Automated Experiments on Ad Privacy Settings", *Proceedings on Privacy Enhancing Technologies*, Vol. 2015/1, pp. 92-112, https://doi.org/10.1515/popets-2015-0007. [149]

Dias, A. et al. (2019), *Referencial de Educação do Consumidor*. [32]

DQUBE Solutions, S. et al. (2020), *Drawing Back The Curtain: Consumer Choice Online in a Data Tracking World*. [154]

Dubé, J., C. Booth and S. Misra (2022), "Personalized Pricing and Consumer Welfare". [138]

Duivenvoorde, B. (2015), *The Consumer Benchmarks in the Unfair Commercial Practices Directive*, Springer International Publishing, Cham, https://doi.org/10.1007/978-3-319-13924-1. [16]

EC (2022), *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation. Final Report*. [95]

EC (2022), *COM(2022)212 final - A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+)*. [93]

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*. [163]

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*. [241]

EC (2018), *Consumer market study on online market segmentation through personalised pricing/offers in the European Union - Final report*, https://doi.org/10.2818/990439. [109]

EC (2018), *Consumers' attitudes towards cross-border trade and consumer protection. Final Report*, https://doi.org/10.2818/209599. [63]

EC (2017), *Study for the Fitness Check of EU consumer and marketing law. Final report*. [173]

EC (2017), *Study on measuring consumer detriment in the European Union Final report Part 1-Main report*. [62]

EC (2016), *Consumer vulnerability across key markets in the European Union: Final report*, https://ec.europa.eu/info/sites/info/files/consumers-approved-report_en.pdf. [25]

EC (2016), *Study on the impact of marketing through social media, online games and mobile applications on children's behaviour*. [55]

EC (2007), *An Analysis of the Issue of Consumer Detriment and the Most Appropriate Methodologies to Estimate It*. [256]

EC (n.d.), *Better Internet for Kids*, https://www.betterinternetforkids.eu/en-GB/home. [193]

EDPS (2021), *Opinion 1/2021 on the Proposal for a Digital Services Act*. [242]

EDRi (2021), *How online ads discriminate. Unequal harms of online advertising in Europe*. [252]

Enke, N. et al. (2021), *Studie zu Werbepraktiken und direkten Kaufappellen an Kinder in sozialen Medien*. [54]

EP (2012), *P7_TA(2012)0209 Strengthening the rights of vulnerable consumers. European Parliament resolution of 22 May 2012 on a strategy for strengthening the rights of vulnerable consumers (2011/2272(INI))*. [178]

EPRS (2021), *Regulating facial recognition in the EU*, https://doi.org/10.2861/140928. [72]

Fallahi and Gascon (2022), *The E-Vulnerability Index*, https://www.canada.ca/en/employment-social-development/corporate/reports/research/e-vulnerability-index.html. [205]

FCA (2022), *A new Consumer Duty. Feedback to CP 21/36 and final rules*. [222]

FCA (2021), *FG21/1 Guidance for firms on the fair treatment of vulnerable customers*. [182]

FCA (2015), *Occasional Paper No.8. Consumer Vulnerability*. [29]

FIAGC (2021), *Consumidor Vulnerable*. [180]

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. [44]

Fletcher, A. et al. (2021), *Consumer Protection for Online Markets and Large Digital Platforms. Policy Discussion Paper No.1*. [77]

Forbrukerrådet (2022), *Insert coin: How the gaming industry exploits consumers using loot boxes*. [85]

Forbrukerrådet (2021), *Time to ban surveillance-based advertising. The case against surveillance online*. [116]

Forbrukerrådet (2020), *Out of Control: How Consumers Are Exploited by the Online Advertising Industry*. [76]

Fussell, S. (2018), "Alexa Wants to Know How You're Feeling Today", *The Atlantic*, https://www.theatlantic.com/technology/archive/2018/10/alexa-emotion-detection-ai-surveillance/572884/. [132]

Gambling Commission (2019), *Young People and Gambling 2019*, https://www.gamblingcommission.gov.uk/statistics-and-research/publication/young-people-and-gambling-2019. [86]

Garrett, D. and P. Toumanoff (2010), "Are Consumers Disadvantaged or Vulnerable? An Examination of Consumer Complaints to the Better Business Bureau", *The Journal of Consumer Affairs*, Vol. 44/1, pp. 3-23, https://doi.org/10.1111/j.1745-6606.2010.01155.x. [65]

Graef, I. (2021), "Consumer Sovereignty and Competition Law: From Personalization to Diversity", *Common Market Law Review*, Vol. 58/2, pp. 471-504, https://doi.org/10.54648/cola2021026. [237]

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. [258]

Greiss, D. (2021), "Addressing digital market manipulation in Australian law", *Australian National University Journal of Law and Technology*, Vol. 2/2. [230]

Hacker, P. (2021), "Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law", *European Law Journal*, https://doi.org/10.1111/EULJ.12389. [131]

Helberger, N., F. Borgesius and A. Reyna (2017), "The perfect match? A closer look at the relationship between EU consumer law and data protection law", *Common Market Law Review*, Vol. 54/5, pp. 1427-1465. [235]

Helberger, N. et al. (2021), *EU CONSUMER PROTECTION 2.0 Structural asymmetries in digital consumer markets*, https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf. [111]

Helberger, N. et al. (2021), "Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability", *Journal of Consumer Policy 2021*, pp. 1-26, https://doi.org/10.1007/S10603-021-09500-5. [13]

Hill, R. and E. Sharma (2020), *Consumer Vulnerability*, Wiley-Blackwell, https://doi.org/10.1002/jcpy.1161. [8]

Hirsch, D. (2020), "From Individual Control to Social Protection: New Paradigms for Privacy Law [105]

in the Age of Predictive Analytics", *Maryland Law Review*, Vol. 79/2, pp. 439-505.

Howells, G., C. Twigg-Flesner and T. Wilhelmsson (2017), *Rethinking EU consumer law*, https://doi.org/10.4324/9781315164830. [172]

Hwang, T. (2020), *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet*, FSG Originals. [266]

IAB Europe (2020), *WHAT WOULD AN INTERNET WITHOUT TARGETED ADS LOOK LIKE?*. [245]

ibi research & trinnovative (2021), *Empirie zu personalisierten Preisen im E-Commerce*. [135]

ICC (2018), *ICC Advertising and Marketing Communications Code*. [195]

ICN (2021), *ICN Project: 'Competition law enforcement at the intersection between competition, consumer protection, and privacy'. Report: Summary of ICN member actions and policy responses to key intersection issues and next steps for the Project*. [239]

ICO (2020), *Age appropriate design: a code of practice for online services*. [192]

ICPEN (2020), *BEST PRACTICE PRINCIPLES: MARKETING PRACTICES DIRECTED TOWARDS CHILDREN ONLINE*. [185]

IHS Markit (2017), *The economic value of behavioural targeting in digital advertising*. [124]

Ingold, D. and S. Soper (2016), *Amazon Doesn't Consider the Race of Its Customers. Should It?*, https://www.bloomberg.com/graphics/2016-amazon-same-day/. [151]

ISO (2022), *ISO 22458:2022(en) Consumer vulnerability — Requirements and guidelines for the design and delivery of inclusive service*, https://www.iso.org/obp/ui/#iso:std:iso:22458:ed-1:v1:en. [184]

Jabłonowska, A. et al. (2018), "Consumer law and artificial intelligence. Challenges to the EU consumer law and policy stemming from the business' use of artificial intelligence. Final report of the ARTSY project", *EUI Working Papers*, Vol. 11. [130]

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. [45]

Jongepier, F. and M. Klenk (eds.) (2022), *Manipulation, Real-Time Profling, and their Wrongs*, Routledge. [229]

Kaptein, M., D. Eckles and J. Davis (2011), "Envisioning persuasion profiles: challenges for public policy and ethical practice", *Interactions*, Vol. 18/5, pp. 66-69, https://doi.org/10.1145/2008176.2008191. [262]

Kennedy, A., K. Jones and J. Williams (2019), "Children as Vulnerable Consumers in Online Environments", *The Journal of Consumer Affairs*, pp. 1478-1506, https://doi.org/10.1111/joca.12253. [88]

KFTC (2018), *KFTC's Regulations on Online Platforms (presentation at OECD workshop "Regulation and competition in light of digitalisation")*, https://www.slideshare.net/OECD-DAF/regulation-and-competition-in-light-of-digitalisation-korean-fair-trade-commission-january-2018-oecd-workshop. [53]

Laux, J., S. Wachter and B. Mittelstadt (2021), "NEUTRALIZING ONLINE BEHAVIOURAL ADVERTISING: ALGORITHMIC TARGETING WITH MARKET POWER AS AN UNFAIR COMMERCIAL PRACTICE", *Common Market Law Review*, Vol. 58/3, pp. 719-750, https://doi.org/10.54648/cola2021048. [227]

Leahy, D. (2022), "Rocking the Boat: Loot Boxes in Online Digital Games, the Regulatory Challenge, and the EU's Unfair Commercial Practices Directive", *Journal of Consumer Policy*, Vol. 45/3, pp. 561-592, https://doi.org/10.1007/s10603-022-09522-7. [82]

Lee, N., P. Resnick and G. Barton (2019), *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*, https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/. [156]

Leerssen, P. et al. (2019), "Platform Ad Archives: Promises and Pitfalls", *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.3380409. [259]

Liu, K. (2019), "A Global Analysis into Loot Boxes: Is It "Virtually" Gambling", *Washington International Law Journal*, Vol. 8/3, p. 763. [190]

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. [94]

Mahdawi, A. (2018), "Uber developing technology that would tell if you're drunk", *The Guardian*, https://www.theguardian.com/technology/2018/jun/11/uber-drunk-technology-new-ai-feature-patent. [133]

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. [257]

Malgieri, G. and J. Niklas (2020), "Vulnerable data subjects", *Computer Law & Security Review*, Vol. 37, p. 105415, https://doi.org/10.1016/J.CLSR.2020.105415. [236]

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. [46]

Manwaring, K. (2018), "Will emerging information technologies outpace consumer protection law? — The case of digital consumer manipulation", *Competition and Consumer Law Journal*, Vol. 26/141, pp. 141-181, https://archive.org/details/advertpshycho00scotrich/. [228]

Marengo, D. and C. Montag (2020), "Digital Phenotyping of Big Five Personality via Facebook Data Mining: A Meta-Analysis", *Digital Psychology*, Vol. 1/1, pp. 52-64, https://doi.org/10.24989/dp.v1i1.1823. [127]

Marotta, V., V. Abhishek and A. Acquisti (2019), "Online Tracking and Publishers' Revenues: An Empirical Analysis", *Working paper*. [267]

Martinez, A. (2018), *The Noisy Fallacies of Psychographic Targeting*, https://www.wired.com/story/the-noisy-fallacies-of-psychographic-targeting/. [128]

Matz, S. et al. (2017), "Psychological targeting as an effective approach to digital mass persuasion", *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 114/48, pp. 12714-12719, https://doi.org/10.1073/pnas.1710966114. [122]

Medietilsynet (2020), *Barn og Medier 202*. [87]

Meyer, M. et al. (2019), "Advertising in Young Children's Apps: A Content Analysis", *Journal of developmental and behavioral pediatrics : JDBP*, Vol. 40/1, pp. 32-39, https://doi.org/10.1097/DBP.0000000000000622. [98]

Mick, D. et al. (eds.) (2011), *Toward a Process Theory of Consumer Vulnerability and Resilience: Illuminating Its Transformative Potential*, Routledge, https://doi.org/10.4324/9780203813256. [18]

Micklitz, H. and M. Namyslowska (2020), *Münchener Kommentar Zum Lauterkeitsrecht, Art. 8 Rdnr. 22.*. [174]

Mik, E. (2016), "The erosion of autonomy in online consumer transactions", *Law, Innovation and Technology*, Vol. 8/1, pp. 1-38, https://doi.org/10.1080/17579961.2016.1161893. [110]

Milano, S. et al. (2021), *Epistemic fragmentation poses a threat to the governance of online targeting*, Nature Research, https://doi.org/10.1038/s42256-021-00358-3. [233]

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. [48]

MUDA (n.d.), *Movimento Pela Utilizacao Digital Ativa*, https://www.muda.pt/. [204]

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/10.1145/3400899.3400901. [144]

National Numeracy (2021), *A new approach to making the UK numerate*. [161]

Neumann, N., C. Tucker and T. Whitfield (2019), "Frontiers: How effective is third-party consumer profiling? evidence from field studies", *Marketing Science*, Vol. 38/6, pp. 918-926, https://doi.org/10.1287/mksc.2019.1188. [126]

OECD (2022), *Companion Document to the OECD Recommendation on Children in the Digital Environment*, OECD Publishing, Paris, https://doi.org/10.1787/a2ebec7c-en. [186]

OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, https://doi.org/10.1787/44f5e846-en. [3]

OECD (2022), "Enhancing online disclosure effectiveness", *OECD Digital Economy Papers*, No. 335, OECD Publishing, Paris, https://doi.org/10.1787/6d7ea79c-en. [79]

OECD (2022), "Measuring financial consumer detriment in e-commerce", *OECD Digital Economy Papers*, No. 326, OECD Publishing, Paris, https://doi.org/10.1787/4055c40e-en. [4]

OECD (2022), *Report on the Implementation of the Recommendation of the Council on High-level Principles on Financial Consumer Protection*. [261]

OECD (2022), "The role of online marketplaces in protecting and empowering consumers: Country and business survey findings", *OECD Digital Economy Papers*, No. 329, OECD Publishing, Paris, https://doi.org/10.1787/9d8cc586-en. [49]

OECD (2021), "Bridging connectivity divides", *OECD Digital Economy Papers*, No. 315, OECD Publishing, Paris, https://doi.org/10.1787/e38f5db7-en. [210]

OECD (2021), *Bridging digital divides in G20 countries*, OECD Publishing, Paris, https://doi.org/10.1787/35c1d850-en. [159]

OECD (2021), "Children in the digital environment: Revised typology of risks", *OECD Digital Economy Papers*, No. 302, OECD Publishing, Paris, https://doi.org/10.1787/9b8f222e-en. [56]

OECD (2021), *Guidelines for Digital Service Providers*. [194]

OECD (2021), *Infographic "Consumers in the Digital and Global Marketplace"*, https://www.oecd.org/digital/consumer/infographic-consumers-digital-global-marketplace.pdf. [34]

OECD (2021), *Recommendation of the Council on Chilrden in the Digital Environment*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389. [23]

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://doi.org/10.1787/1ce1de63-en. [231]

OECD (2020), *OECD Digital Economy Outlook 2020*, OECD Publishing, Paris, https://doi.org/10.1787/bb167041-en. [69]

OECD (2020), "Protecting children online: An overview of recent developments in legal frameworks and policies", *OECD Digital Economy Papers*, No. 295, OECD Publishing, Paris, https://doi.org/10.1787/9e0e49a9-en. [57]

OECD (2020), *Protecting online consumers during the Covid-19 crisis*, https://www.oecd.org/coronavirus/policy-responses/protecting-online-consumers-during-the-covid-19-crisis-2ce7353c/. [37]

OECD (2020), *Recommendation of the Council on Consumer Product Safety*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0459. [24]

OECD (2020), *Roundtable on Redress for Non-monetary Transactions: Summary of discussion*. [81]

OECD (2019), *Artificial Intelligence in Society*, OECD Publishing, Paris, https://doi.org/10.1787/eedfee77-en. [150]

OECD (2019), *Challenges to Consumer Policy in the Digital Age*, https://www.oecd.org/sti/consumer/challenges-to-consumer-policy-in-the-digital-age.pdf. [2]

OECD (2019), "Good practice guide on consumer data", *OECD Digital Economy Papers*, No. 290, OECD Publishing, Paris, https://doi.org/10.1787/e0040128-en. [191]

OECD (2019), "Good practice guide on online advertising: Protecting consumers in e-commerce", *OECD Digital Economy Papers*, No. 279, OECD Publishing, Paris, https://doi.org/10.1787/9678e5b1-en. [52]

OECD (2019), "Good practice guide on online consumer ratings and reviews", *OECD Digital Economy Papers*, No. 288, OECD Publishing, Paris, https://doi.org/10.1787/0f9362cf-en. [58]

OECD (2019), "Online advertising: Trends, benefits and risks for consumers", *OECD Digital Economy Papers*, No. 272, OECD Publishing, Paris, https://doi.org/10.1787/1f42c85d-en. [51]

OECD (2019), *Recommendation of the Council on Artificial Intelligence*, https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449. [246]

OECD (2019), *Report on the Implementation of the Recommendation of the Council on Consumer Policy Decision-making*. [162]

OECD (2019), *Roundtable on Digital Assistants and Voice-Controlled e-commerce: Summary of discussion*. [68]

OECD (2019), *WHAT DO WE KNOW ABOUT CHILDREN AND TECHNOLOGY?*, https://www.oecd.org/education/ceri/Booklet-21st-century-children.pdf. [89]

OECD (2018), "Bridging the rural digital divide", *OECD Digital Economy Papers*, No. 265, OECD Publishing, Paris, https://doi.org/10.1787/852bd3b9-en. [157]

OECD (2018), "Consumer policy and the smart home", *OECD Digital Economy Papers*, No. 268, OECD Publishing, Paris, https://doi.org/10.1787/e124c34a-en. [71]

OECD (2018), "Improving online disclosures with behavioural insights", *OECD Digital Economy Papers*, No. 269, OECD Publishing, Paris, https://doi.org/10.1787/39026ff4-en. [201]

OECD (2018), *Personalised Pricing in the Digital Era - Background Note by the Secretariat*. [104]

OECD (2018), *Quality considerations in digital zero-price markets - Background Note by the Secretariat*. [78]

OECD (2018), *Toolkit for protecting digital consumers: A resource for G20 policy makers*. [35]

OECD (2016), *OECD Recommendation of the Council on Consumer Protection in E-Commerce*, OECD Publishing, Paris, https://doi.org/10.1787/9789264255258-en. [22]

OECD (2016), "Online Product Safety Sweep Results: Australian Competition and Consumer Commission", *OECD Digital Economy Papers*, No. 262, OECD Publishing, Paris, https://doi.org/10.1787/5jlnb5q64ktd-en. [67]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, https://doi.org/10.1787/9789264229358-en. [103]

OECD (2014), "Consumer Policy Guidance on Mobile and Online Payments", *OECD Digital Economy Papers*, No. 236, OECD Publishing, Paris, https://doi.org/10.1787/5jz432cl1ns7-en. [70]

OECD (2014), *Recommendation on Consumer Policy Decision Making*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0403. [21]

OECD (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. [234]

OECD (2010), *Consumer Policy Toolkit*, OECD Publishing, Paris, https://doi.org/10.1787/9789264079663-en. [1]

OECD (2007), *Recommendation on Consumer Dispute Resolution and Redress*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0356. [19]

OECD (1999), *Guidelines for Consumer Protection in the Context of Electronic Commerce*. [260]

OECD (forthcoming), *2021 Online product safety sweep*. [66]

Ofcom (2014), *The Communications Market Report*. [91]

Office of the eSafety Commissioner (2018), *Understanding digital behaviour amongst adults aged 50 years and over*. [61]

Ofgem (2013), *Consumer Vulnerability Strategy*. [30]

Paterson, J. et al. (2021), "The Hidden Harms of Targeted Advertising by Algorithm and Interventions from the Consumer Protection Toolkit", *International Journal on Consumer Law and Practice*, Vol. 9, pp. 1-24. [115]

Poort, J. and F. Borgesius (2019), "Does everyone have a price? Understanding people's attitude towards online and offline price discrimination", *Internet Policy Review*, Vol. 8/1, https://doi.org/10.14763/2019.1.1383. [140]

PROFECO (2020), *Think about it before you click!*, https://www.gob.mx/cms/uploads/attachment/file/591181/PATRONES_OSCUROS_COMPRAR_EN_INTERNER.pdf. [207]

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. [99]

Rahman, K. and Z. Teachout (2020), *From Private Bads to Public Goods: Adapting Public Utility Regulation for Informational Infrastructure*, https://knightcolumbia.org/content/from-private-bads-to-public-goods-adapting-public-utility-regulation-for-informational-infrastructure. [244]

Riedel, A. et al. (2021), "Consumers experiencing vulnerability: a state of play in the literature", *Journal of Services Marketing*, https://doi.org/10.1108/JSM-12-2020-0496. [255]

Riefa, C. (2020), "Coronavirus as a Catalyst to Transform Consumer Policy and Enforcement", *Journal of Consumer Policy*, Vol. 43/3, pp. 451-461, https://doi.org/10.1007/s10603-020-09462-0. [43]

Riefa, C. (2020), *THE PROTECTION OF VULNERABLE CONSUMERS IN THE DIGITAL AGE*, https://ec.europa.eu/info/sites/info/files/consumers-approved-report_en.pdf. [26]

Riefa, C. and S. Saintier (eds.) (2020), *A universal perspective on vulnerability. International definitions and targets*, Routledge. [36]

Riefa, C. and S. Saintier (eds.) (2020), *Economic theory and consumer vulnerability. Exploring and uneasy relationship*, Routledge. [171]

Riefa, C. and S. Saintier (eds.) (2020), *The legal definition of 'vulnerable' consumers in the UCPD: Benefits and limitations of a focus on personal attributes*, Routledge. [7]

Riefa, C. and S. Saintier (2020), *Vulnerable consumers and the law: Consumer protection and access to justice*, https://doi.org/10.4324/9781003104650. [211]

Rosen, R. (2013), "Is This the Grossest Advertising Strategy of All Time?", *The Atlantic*, https://www.theatlantic.com/technology/archive/2013/10/is-this-the-grossest-advertising-strategy-of-all-time/280242/. [117]

Rotzmeier-Keuper, J. (2020), "Consumer Vulnerability: Overview and Synthesis of the Current State of Knowledge and Future Service-Related Research Directions", https://ideas.repec.org/p/pdn/dispap/65.html. [6]

Satarino, A. (2021), "What a Gambling App Knows About You", *New York Times*, https://www.nytimes.com/2021/03/24/technology/gambling-apps-tracking-sky-bet.html. [118]

SERNAC (2021), *Circular Interpretativa sobre noción de consumidor hipervulnerable*. [33]

Shiller, B. (2014), *First-Degree Price Discrimination Using Big Data*, https://econpapers.repec.org/paper/brdwpaper/58.htm. [137]

Shultz, C. and M. Holbrook (2009), "The Paradoxical Relationships Between Marketing and Vulnerability", *Journal of Public Policy & Marketing*, Vol. 28/1, pp. 1547-7207. [10]

Siciliani, P., C. Riefa and H. Gamper (2019), *Consumer Theories of Harm. An economic approach to consumer law enforcement and policy making*, Hart. [75]

Smith, N. and E. Cooper-Martin (1997), "Ethics and Target Marketing: The Role of Product Harm and Consumer Vulnerability", *Journal of Marketing*, Vol. 61/3, p. 1, https://doi.org/10.2307/1251786. [5]

Spencer, S. (2020), *The problem of online manipulation*, https://doi.org/10.2139/ssrn.3341653. [101]

Steinberg, L. (2007), *Risk taking in adolescence: new perspectives from brain and behavioral science*. [92]

Stigler Committee (2019), *Final Report*, https://www.chicagobooth.edu/research/stigler/news-and-media/committee-on-digital-platforms-final-report. [148]

Strycharz, J. and B. Duivenvoorde (2021), "The exploitation of vulnerability through personalised marketing communication: Are consumers protected?", *Internet Policy Review*, Vol. 10/4, https://doi.org/10.14763/2021.4.1585. [108]

Strycharz, J. et al. (2021), "No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies", *Computers in Human Behavior*, Vol. 120, p. 106750, https://doi.org/10.1016/J.CHB.2021.106750. [232]

Subscribed Institute (2021), *The End of Ownership Report*. [74]

Subscribed Institute (2021), *The Subscription Economy Index*. [73]

Sweeney, L. (2013), "Discrimination in Online Ad Delivery", *SSRN Electronic Journal*, https://doi.org/10.2139/SSRN.2208240. [152]

Tiki, N. (2017), "Get Ready for the Next Big Privacy Backlash Against Facebook", *Wired*, https://www.wired.com/2017/05/welcome-next-phase-facebook-backlash/. [119]

Turow, J. et al. (2011), "Americans Reject Tailored Advertising and Three Activities that Enable It", *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.1478214. [123]

UK BEIS (2021), *Smart Data Working Group: Spring 2021 report*. [219]

UK DBT & DSIT (2023), *Enhancing consumer rights: policy summary briefing. Digital Markets, Competition and Consumers Bill*. [50]

UK DCMS (2020), *Loot Boxes in Video Games. Call for Evidence*. [83]

UNCRC (2021), *General comment No. 25 (2021) on children's rights in relation to the digital environment*. [187]

UNCTAD (ed.) (2021), *CONSUMER LAW ENFORCEMENT AS A TOOL TO BOLSTER COMPETITION IN DIGITAL MARKETS: A CASE STUDY ON PERSONALIZED PRICING*. [226]

UNCTAD (2018), *Working Group on Vulnerable and Disadvantaged Consumers*. [181]

UNCTAD (2015), *United Nations Guidelines for Consumer Protection*. [20]

US DOJ (2022), *"Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising", media release, 21 June 2022*, https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known. [249]

US FTC (2023), *Negative Option Rule*, https://www.federalregister.gov/documents/2023/04/24/2023-07035/negative-option-rule. [217]

US FTC (2022), *Bringing Dark Patterns to Light*, https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf. [225]

US FTC (2022), *Combatting Online Harms Through Innovation*, https://www.ftc.gov/reports/combatting-online-harms-through-innovation. [224]

US FTC (2022), *Trade Regulation Rule on Commercial Surveillance and Data Security*, https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security. [218]

US FTC (2022), *Trade Regulation Rule on the Use of Reviews and Endorsements*, https://www.federalregister.gov/documents/2022/11/08/2022-24139/trade-regulation-rule-on-the-use-of-reviews-and-endorsements. [216]

US FTC (2022), *Unfair or Deceptive Fees Trade Regulation Rule Commission Matter No. R207011*, https://www.federalregister.gov/documents/2022/11/08/2022-24326/unfair-or-deceptive-fees-trade-regulation-rule-commission-matter-no-r207011. [215]

US FTC (2021), *Enforcement Policy Statement Regarding Negative Option Marketing*. [168]

US FTC (2021), *Protecting Older Consumers 2020-2021*. [40]

US FTC (2021), *Serving Communities of Color. A Staff Report on the Federal Trade Commission's Efforts to Address Fraud and Consumer Issues Affecting Communities of Color*. [253]

US FTC (2020), *Daily COVID-19 Complaint Data*, https://public.tableau.com/app/profile/federal.trade.commission/viz/COVID-19andStimulusReports/Map. [38]

US FTC (2020), *Using Artificial Intelligence and Algorithms*, https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms. [248]

US FTC (2018), *Net Cetra*, https://www.bulkorder.ftc.gov/publications/net-cetera-chatting-kids-about-being-online. [209]

US FTC (2010), *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid- [177]

change-proposed-framework.

US FTC (1984), *FTC Policy Statement on Deception. Appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984).*. [164]

US FTC (n.d.), *OnGuard Online*, https://www.ftc.gov/consumers/onguard-online. [208]

US FTC (n.d.), *Pass It On*, https://consumer.ftc.gov/features/pass-it-on. [202]

Vedantam, S. and M. Penman (2016), *This Is Your Brain On Uber*, https://www.npr.org/2016/05/17/478266839/this-is-your-brain-on-uber. [141]

Wachter, S. (2019), "Affinity Profiling and Discrimination by Association in Online Behavioural Advertising", *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.3388639. [251]

Wagner, G. and H. Eidenmüller (2019), *Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions*, http://perma.cc/V94Y-T7F3. [139]

Webb, K. et al. (2020), *"Context is all": Court confirms test and principles for false, misleading or deceptive conduct*, https://www.claytonutz.com/knowledge/2020/october/context-is-all-court-confirms-test-and-principles-for-false-misleading-or-deceptive-conduct. [166]

Weinzierl, Q. (2020), *Dark Patterns als Herausforderung für das Recht*. [146]

Williams, S. (2022), *Targeted Advertising: Does it Actually Work?*, https://contently.com/2022/02/09/targeted-advertising-does-it-actually-work/. [125]

Willis, L. (2020), "Deception by Design", *Harvard Journal of Law & Technology*, Vol. 34/1, https://ssrn.com/abstract=3694575. [47]

Willis, L. (2017), "PERFORMANCE-BASED REMEDIES: ORDERING FIRMS TO ERADICATE THEIR OWN FRAUD", *LAW & CONTEMPORARY PROBLEMS*, Vol. 80/3, pp. 7-41, https://ssrn.com/abstract=3018168Electroniccopyavailableat:https://ssrn.com/abstract=3018168. [212]

Willis, L. (2015), "Performance-based consumer law", *University of Chicago Law Review*, Vol. 82, p. 1309. [176]

Woodcock, R. (2018), "The obsolescence of advertising in the information age", *Yale Law Journal*, Vol. 127/8, pp. 2270-2341. [243]

Yeung, K. (2017), "'Hypernudge': Big Data as a mode of regulation by design", *Information Communication and Society*, Vol. 20/1, pp. 118-136, https://doi.org/10.1080/1369118X.2016.1186713. [145]

Zang, J. (2021), *Solving the problem of racially discriminatory advertising on Facebook*, https://www.brookings.edu/research/solving-the-problem-of-racially-discriminatory-advertising-on-facebook/. [153]

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. [113]

Zendle et al (2020), *The prevalence of loot boxes in mobile and desktop games*, https://doi.org/10.1111/add.14973. [84]

Zuiderveen Borgesius, F. (2020), "Price discrimination, algorithmic decision-making, and European non-discrimination law", *European Business Law Review*, Vol. 31/3, pp. 401-422, https://doi.org/10.54648/eulr2020017. [250]

Zuiderveen Borgesius, F. (2018), *Discrimination, Artificial intelligence and Algorithmic Decision-making*. [247]

Notes

[1] See https://www.oecd.org/sti/consumer/34023811.pdf.

[2] See https://www.oecd.org/daf/competition/workshop-on-applying-behavioural-insights-to-consumer-and-competition-policy.htm for further details, including the issues paper supporting the workshop.

[3] The concept of "disadvantaged consumer" was originally coined by Andreasen (1975[266]) to characterise difficulties faced by consumers in urban ghettos, particularly the poor, racial minorities, the elderly, the uneducated and the non-English speaking.

[4] Though it should be noted that this is a revision of a principle featuring in the prior 1999 Guidelines for Consumer Protection in the Context of Electronic Commerce – *"Businesses should take special care in advertising or marketing that is targeted to children, the elderly, the seriously ill, and others who may not have the capacity to fully understand the information with which they are presented"* (OECD, 1999[277]), which may implicitly suggest that the elderly and seriously ill are considered vulnerable or disadvantaged groups.

[5] OECD calculations based on the OECD ICT Access and Usage by Households and Individuals database at http://oe.cd/hhind.

[6] See https://www.reviews.org/au/reviews/fake-reviews-survey/.

[7] See e.g. https://rytr.me/use-cases/testimonial-review-generator.

[8] See https://www.which.co.uk/news/article/fake-ads-real-problems-how-easy-is-it-to-post-scam-adverts-on-google-and-facebook-aBRVx1e3HVF5.

[9] See https://injuryfacts.nsc.org/home-and-community/safety-topics/consumer-product-injuries/data-details/.

[10] In this context, the CCP's WPCPS is developing a methodological project over 2023-2024 on approaches to measuring the costs of unsafe products.

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

[12] The EU General Data Protection Regulation, Article 4, defines profiling as *"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's*

performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

[13] Some commentators distinguish personalisation and individualisation, where the latter is used to describe personalisation at the individual level (Jabłonowska et al., 2018[129]).

[14] For more information on how online advertising works, see the CCP's report on the topic (OECD, 2019[50]).

[15] See https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[16] See https://www.theguardian.com/technology/2021/apr/28/facebook-allows-advertisers-to-target-children-interested-in-smoking-alcohol-and-weight-loss.

[17]See e.g. https://www.abc.net.au/news/2019-07-13/searches-data-mined-by-pharma-giant-to-promote-new-opioid/11300396.

[18] See e.g. https://edition.cnn.com/2018/04/10/health/facebook-likes-psychographics/index.html.

[19] According to Hwang (2020[268]), key factors that may compromise effectiveness of targeted advertising include ineffectual placement, consumer ad blocking and click fraud (use of automated scripts of paid humans to click on ads). See also research suggesting that often ad publishers do not benefit from targeted advertising, e.g. Marotta, Abhishek and Acquisti (2019[270]) and https://digiday.com/media/digiday-research-most-publishers-dont-benefit-from-behavioral-ad-targeting/.

[20] A persuasion profile has been described as *"sets of estimates on the effectiveness of particular influence-strategies on individuals, based on their past responses to these strategies"* (Kaptein, Eckles and Davis, 2011[290]).

[21] Over 2023-2024, the CCP is developing a project involving a review of initiatives using AI to identify and mitigate consumer risks online.

[22] See e.g. https://themarkup.org/citizen-browser/2021/04/29/credit-card-ads-were-targeted-by-age-violating-facebooks-anti-discrimination-policy for an example of direct age-based discrimination.

[23] According to Datta et al. (2018[264]), when an advertising algorithm uses a targeting criterion because it is known to correlate with certain characteristics (which may be protected), that criterion is a "proxy". Examples are using "interest in LGTBQI issues" or "menstrual apps" as a means to target people who identify as LGBTQ or women respectively (EDRi, 2021[254]).

[24] Regarding reports of care insurance price discrimination, for the United States see e.g. https://consumerfed.org/wp-content/uploads/2020/01/Summary-of-Auto-Insurance-Research.pdf or https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk ; for Canada see e.g. https://www.thestar.com/news/gta/2019/03/10/your-postal-code-is-a-big-factor-in-determining-your-car-insurance-rates-critics-say-it-shouldnt-be.html ; for the Netherlands see e.g. https://www.consumentenbond.nl/autoverzekering/je-postcode-en-de-premie.

[25] See https://www.canada.ca/en/employment-social-development/corporate/reports/research/e-vulnerability-index.html.

[26] See Richard v. Time at https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/7994/index.do.

[27] The US FTC has also previously evaluated a claim from the perspective of the "average listener" (US FTC, 1984[165]), suggesting that the terms "average" and "reasonable" may in some cases be interchangeable.

[28] See UCPD, Articles 5(2) and 5(3) and Recital 18; see also European Court of Justice, Case C-210/96 Gut Springenheideand Tusky[1998] ECR I-4657, paragraph 31.

[29] See Richard v. Time at https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/7994/index.do.

[30] See https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/full/2021/2021fcafc0142.

[31] See https://elaw.klri.re.kr/kor_service/lawView.do?hseq=49238&lang=ENG.

[32] The Common Market Group of Mercosur Resolution 11/2021 furthermore indicates that the following may constitute causes of hyper-vulnerability: a) being a child or adolescent; b) being an elderly person in accordance with the Inter-American Convention on the Protection of the Human Rights of Older Persons; c) being a person with a disability; d) having the status of migrant person; e) having the status of a tourist; f) belonging to indigenous communities, native peoples or ethnic minorities; g) being in a situation of socio-economic vulnerability; h) belonging to a single-parent family in charge of underage or disabled children; i) having serious health problems.

Mercosur member states are required to adopt measures to a) favour effective and expeditious procedures for the appropriate resolution of disputes of hyper-vulnerable consumers; b) eliminate or mitigate obstacles to access to justice for hyper-vulnerable consumers; c) implement policies of guidance, advice, assistance and support for hyper-vulnerable consumers in the filing of claims in the framework of consumer relations; d) adapt administrative or judicial procedures for the full exercise of the rights of hyper-vulnerable consumers; e) implement actions of education, dissemination, information and differentiated protection for hyper-vulnerable consumers; f) encourage communication with clear, colloquial language, expressed in plain, concise, understandable and appropriate to the conditions of hyper vulnerable consumers; g) promote accessibility in the communication and information channel to the consumer; h) promote, among suppliers of goods and services, good commercial practices in terms of attention, treatment and protection of the rights of hyper-vulnerable consumers; i) protect hyper-vulnerable consumers from misleading or abusive advertising and offers; j) promote the protection of data and privacy of hyper vulnerable consumers.

[33] See http://www.consumeracademy.gov.tr/data/58bd652f1a79f7ea0857d910/COMMERCIAL%20ADVERTISING%20AND%20UNFAIR%20COMMERCIAL%20PRACTICES.doc.

[34] As part of the review of the implementation of the G20/OECD High-Level Principles on Financial Consumer Protection, 34 jurisdictions reported that there are some standards or requirements in place for enhanced protections for consumers experiencing financial hardship or financial services-related vulnerability. For more discussion of measures in different jurisdictions on this topic, see OECD (2022[262]). For discussion of measures addressing energy sector vulnerability and financial hardship in the European Union, see EC (2016[25]).

[35] See https://unctad.org/topic/competition-and-consumer-protection/consumer-protection-map.

[36] See https://cdn.opc.gouv.qc.ca/media/documents/consommateur/sujet/publicite-pratique-illegale/EN_Guide_publicite_moins_de_13_ans_vf.pdf?1379441297.

[37] See https://www.caa.go.jp/policies/policy/representation/fair_labeling/faq/card/.

[38] See http://www.consumeracademy.gov.tr/data/58bd652f1a79f7ea0857d910/COMMERCIAL%20ADVERTISING%20AND%20UNFAIR%20COMMERCIAL%20PRACTICES.doc.

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

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

[41] See https://www.cnil.fr/fr/la-cnil-publie-8-recommandations-pour-renforcer-la-protection-des-mineurs-en-ligne.

[42] Gemeinsame Richtlinien der Landesmedienanstalten zur Gewährleistung des Schutzes der Menschenwürde und des Jugendschutzes. See https://www.kjm-online.de/fileadmin/user_upload/Rechtsgrundlagen/Richtlinien_Leitfaeden/JuschRiLi_der_Landesmedienanstalten_ab_15.10.2019.pdf.

[43] See Press Release, Children's Advertising Review Unit Issues Revised Guidelines for Responsible Advertising to Children, Effective January 1, 2022 (July 29, 2021) at https://bbbprograms.org/media-center/news/CARU-revised-guidelines-for-advertising-to-children.

[44] See https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273 for further details.

[45] See https://crsreports.congress.gov/product/pdf/LSB/LSB10776.

[46] See https://www.parl.ca/legisinfo/en/bill/44-1/c-27.

[47] See https://www.fieldfisher.com/en/insights/update-netherlands-and-spain-propose-tighter-regulation-on-loot-boxes.

[48] See https://www.congress.gov/bill/116th-congress/senate-bill/1629/text.

[49] The FTC convened the first meeting of this advisory group in September 2022. See https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-convene-first-meeting-scams-against-older-adults-advisory-group-sept-29.

[50] See https://news.mynavi.jp/article/20211007-2024038/.

[51] See https://www.cas.go.jp/jp/seisaku/digital_denen/pdf/20220607_honbun.pdf.

[52] See https://www.caa.go.jp/policies/policy/consumer_policy/information/notice/assets/efforts_004_200825_0003.pdf.

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

[54] See https://www.dentons.com/en/insights/articles/2020/october/8/the-new-cancelation-link; https://www.jdsupra.com/legalnews/new-two-click-cancellation-button-4437257/ ; see https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800; The German government furthermore indicated that it would advocate at EU level for electronic cancellation buttons to become mandatory; require provision of information on average monthly costs for continuing obligations for the delivery of goods or the regular provision of services and goods; and require subscription contracts to always be offered with a minimum term of no more than one year.

[55] Restore Online Shoppers' Confidence Act, 15 U.S.C. §§ 8401-8405.

[56] See https://www.gov.uk/government/news/new-bill-to-crack-down-on-rip-offs-protect-consumer-cash-onlineand-boost-competition-in-digital-markets.

[57] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules.

[58] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rule.

[59] See https://crsreports.congress.gov/product/pdf/LSB/LSB10776.

[60] See https://www.parl.ca/legisinfo/en/bill/44-1/c-27.

[61] See https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988.

[62] See https://www.ftc.gov/news-events/events/2022/09/commercial-surveillance-data-security-anpr-public-forum.

[63] See https://www.consilium.europa.eu/en/press/press-releases/2023/04/25/council-gives-final-green-light-to-legislation-that-will-make-products-safer-for-consumers/.

[64] See https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

[65] See https://www.gov.uk/government/news/major-law-changes-to-protect-people-from-scam-adverts-online.

[66] For the United Kingdom see https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum ; for the Netherlands see https://www.acm.nl/en/about-acm/cooperation/national-

cooperation/digital-regulation-cooperation-platform-sdt; for Australia see https://www.acma.gov.au/dp-reg-joint-public-statement.

[67]See https://www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1.

[68] A related concept proposed for privacy law is the concept of an "information fiduciary", described as a duty to use personal data in ways that do not betray end users and harm them (Balkin and Zittrain, 2016[293]).

[69] Over 2023-2024, the CCP is developing a project involving a review of initiatives using AI to identify and mitigate consumer risks online.

[70] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules.

[71] Prohibitions on unconscionable conduct in the Australian Consumer Law (Schedule 2 of the Competition and Consumer Act 2010) and Australian Securities and Investments Commission Act 2001 have been used to challenge a business practice that targets a consumer's vulnerability or disadvantage, though scholars consider that the prohibition may set too high a bar to address more subtle personalised advertising exploiting vulnerabilities (Manwaring, 2018[228]; Paterson et al., 2021[115]).

[72] The EC also notes that a dynamic pricing practice where a business raises a price after the consumer has put the product in their digital shopping cart or proceeds to payment, without giving the consumer reasonable time to complete the transaction, could be considered contrary to professional diligence or as an aggressive practice under Articles 8 and 9 of the UCPD (EC, 2021[164]).

[73] In this regard, the CCP and the OECD Competition Committee held a joint workshop in April 2023 on behavioural insights in consumer and competition policy, with a focus on dark patterns and exploitative personalisation practices and the consumer and competition policy and law tools to address them. See https://www.oecd.org/daf/competition/workshop-on-applying-behavioural-insights-to-consumer-and-competition-policy.htm for details.

[74] See https://crsreports.congress.gov/product/pdf/LSB/LSB10776 and https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading.

[75] See https://www.eff.org/de/issues/do-not-track.

[76] In draft amendments proposed at the time of writing by the European Parliament's Committee on the Internal Market and Consumer Protection and Committee on Civil Liberties, Justice and Home Affairs, a prohibition on AI systems that exploit a broader set vulnerabilities was proposed, namely *"any of the vulnerabilities of a person or a specific group of persons, including characteristics of such individual's or group of persons' known or predicted personality traits or social or economic situation, age, physical or mental ability".* See https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence.

[77] For example, US law prohibits discrimination against protected classes in credit (https://www.law.cornell.edu/uscode/text/15/1691), housing (https://www.law.cornell.edu/uscode/text/42/3604), and health care and health insurance (https://www.law.cornell.edu/uscode/text/42/18116). See also https://www.brookings.edu/research/fairness-in-algorithmic-decision-making/.

[78] See e.g. Facebook's (https://www.facebook.com/policies_center/ads) and Google's (https://support.google.com/adspolicy/answer/6008942?hl=en&visit_id=637202367689914083-1486308337&rd=1) policies, and recent updates to the latter (https://www.blog.google/technology/ads/upcoming-update-housing-employment-and-credit-advertising-policies/).

[79] For example, according to Zuiderveen Borgesius (2020[250]) EU non-discrimination law does not prohibit price discrimination on the basis of religion or belief, disability, age or sexual orientation.

[80] See e.g. Zuiderveen Borgesius (2018[247]), who notes that in the European Union the prohibition of indirect discrimination does not provide a clear and easily applicable rule, and that the concept of indirect discrimination results in rather open-ended standards, which are often difficult to apply in practice. It may also be unclear to what extent differential treatment is discriminatory: see e.g. Jabłonowska et al. (2018[130]), who note, in relation to discriminatory outcomes of algorithmic advertising: "*If 51% of a job's ad audience is white male, is that discrimination already? 60%? 90%?".*

[81] See https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

[82] For example, as reported, by the ACCC (2019[80]), the Attorney-General of the US state of Washington conducted an investigation under the unfair acts and practices provisions of its consumer law, resulting in a legally binding agreement with Facebook to discontinue "discriminatory" advertising categories. See https://www.atg.wa.gov/news/news-releases/ag-ferguson-investigation-leads-facebook-making-nationwide-changes-prohibit for details.

[83] Under the Dodd-Frank Act, *"an act or practice is unfair when: 1) It causes or is likely to cause substantial injury to consumers; 2) The injury is not reasonably avoidable by consumers; and 3) The injury is not outweighed by countervailing benefits to consumers or to competition."* The US Consumer Financial Protection Bureau (CFPB) explains how discrimination from a biased algorithm could in theory satisfy all three of those requirements (CFPB, 2022[254]).

[84] See https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai for details. In draft amendments proposed to the EC's draft AIA Act at the time of writing by the European Parliament's Committee on the Internal Market and Consumer Protection and Committee on Civil Liberties, Justice and Home Affairs, a prohibition was furthermore suggested on AI systems that *"categorise natural persons according to sensitive or protected attributes or characteristics or based on the inference of those attributes or characteristics".* See https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence.

[85] See https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading.

[86] See https://crsreports.congress.gov/product/pdf/LSB/LSB10776.

[87] The CCP is developing empirical work on dark patterns and how they affect consumer vulnerability over 2023-2024, taking into account the gaps in evidence and methods described in this section. Many of the methods described will also be further explored in the methodological project the CCP is developing over 2023-2024 on approaches to measuring the impact of consumer policy interventions (such as different remedies addressing specific consumer risks highlighted in this report).

[88] A mixed method approach is often adopted in EC consumer evidence studies, which often incorporate a consumer survey, behavioural experiment and mystery shopping.