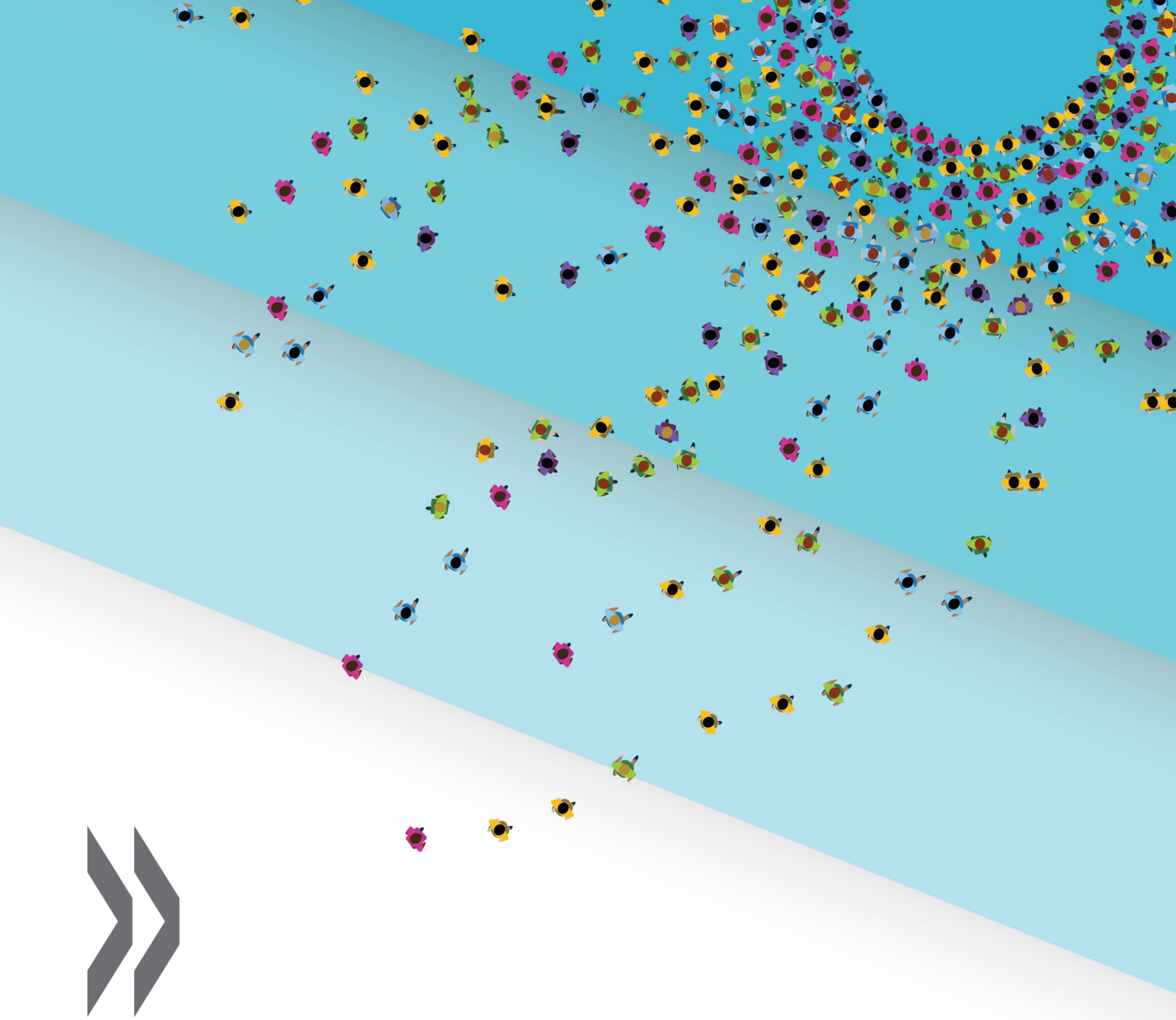


Protecting and empowering consumers in the digital transition

ISSUES NOTE

Consumer Policy
Ministerial Meeting

Consumers at the
centre of the digital
and green transitions

OECD
BETTER POLICIES FOR BETTER LIVES

This provides background information for discussion at the
OECD Consumer Policy Ministerial Meeting.

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD Member countries.

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

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

Photo credit: Shutterstock and Adobe Stock

KEY POINTS

Digital markets offer easy access to goods, services, and information, and digital technologies hold the promise of improving consumers' lives. But many of these markets are not functioning such that consumers can realise their full benefits. Digital business models and technologies can create and exacerbate information and structural power asymmetries, facilitating business practices that can mislead and exploit consumers. This weakens consumer choice and trust, and forces honest businesses to compete on an uneven playing field.

OECD empirical work highlights how many consumers experience problems online and how their decisions can be significantly influenced by manipulative online design techniques to their detriment. Other risks include fake reviews, exploitative personalisation, pervasive and extensive data collection, tracking and sharing, the exploitation of behavioural biases, algorithmic discrimination, fraud and scams. All consumers may be vulnerable to such practices and some groups, defined for example by age or gender, may face particular risks. The consequences include wide-ranging consumer harm, ranging from financial loss, erosion of privacy to psychological harm.

A strong and effective consumer policy environment enables consumers to have trust in digital markets. Many consumer authorities have taken action against harmful digital practices. However, there are concerns about whether existing laws and enforcement mechanisms are sufficiently effective and efficient to address digital harms, and in some jurisdictions new laws have been introduced. As digital consumer risks are borderless and cut across policy areas, international and interdisciplinary co-operation is needed.

THE DIGITAL TRANSITION: A DOUBLE-EDGED SWORD FOR CONSUMERS

The digital transition has profoundly changed consumers’ interaction with the marketplace. Well-functioning digital markets can benefit consumers through easy access to a wide range of goods and services and more complete information to make informed decisions. Digital technologies, such as artificial intelligence (AI), Internet of Things (IoT) and virtual reality, hold the promise of improving consumers’ lives.

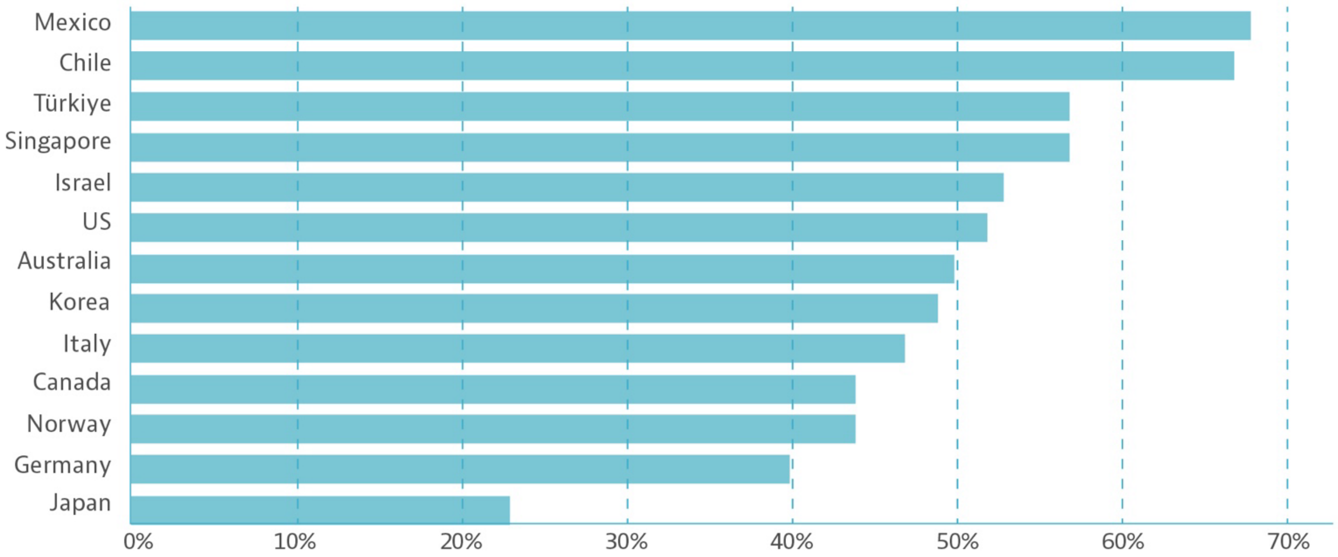
However, the benefits of digital markets also bear downsides. The distance-selling nature of e-commerce exposes consumers to unreliable indicators of quality or safety (e.g. fake reviews, undisclosed influencer sponsorships), unfamiliar and often deliberately challenging transaction types (e.g. subscription traps, paying with personal data, or obscure microtransactions), and greater hurdles in obtaining redress for problems. And while many problems online also occur in physical stores (e.g. products not functioning as advertised), their prevalence and severity can be substantially amplified online.

A 2021 OECD survey conducted across 13 countries revealed that on average 50% of online consumers faced at least one problem in e-commerce in the prior year, including unfair or misleading practices, scams and fraud.[1]

Taking into account only their most serious problem, and accounting for any redress they received, consumers in OECD countries were estimated to lose a total of USD 22 billion in 2020; in some countries losses amounted to 3% of total e-commerce sales for that year.[1] In addition to emotional stress, time lost dealing with the problem (five hours on average), represented an additional loss of USD 15 billion in monetary terms.

[1] 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

Figure 1. **Online transaction problem frequency (2020)**



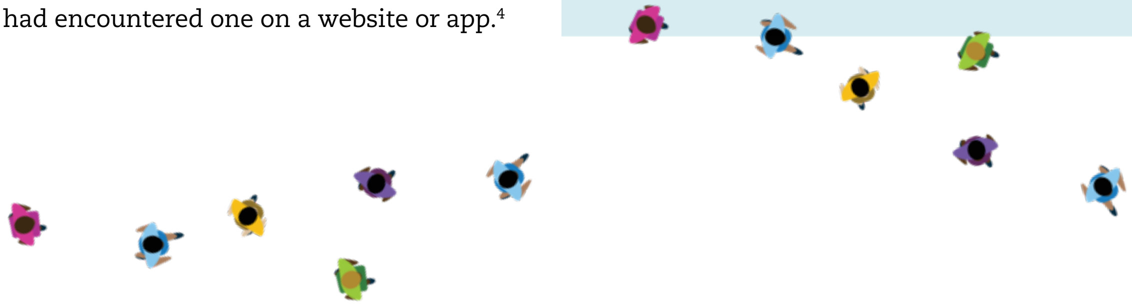
Source: OECD (2022), “Measuring financial consumer detriment in e-commerce”, *OECD Digital Economy Papers*, No. 326, OECD Publishing, Paris, https://doi.org/10.1787/4055c40e-en

Digital business models can also intensify information and power asymmetries, which can facilitate practices that mislead and exploit consumers, and ultimately weaken consumer choice and trust in markets. Specifically, businesses can more readily capitalise on consumer behaviour patterns online in order to shape digital designs in ways that can harm consumers.[2] The pervasive data collection from consumers’ interaction with digital products and services, including via repeated experiments (or “A/B testing”), further enables businesses to not only invasively track and profile consumers extensively – with the ensuing privacy risks – but also exploit behavioural biases more precisely. Indeed, well-honed manipulative, coercive, deceptive or addictive online design techniques known as dark commercial patterns are alarmingly widespread.[3] A 2024 OECD study across 20 countries revealed 9 in 10 consumers had encountered one on a website or app.[4]

A 2024 OECD study across 20 countries revealed

9 in 10 consumers

had encountered a dark pattern on a website or app.[4]



[2] OECD (2023), “Consumer vulnerability in the digital age”, *OECD Digital Economy Papers*, No. 355, OECD Publishing, Paris, https://doi.org/10.1787/4d013cc5-en.

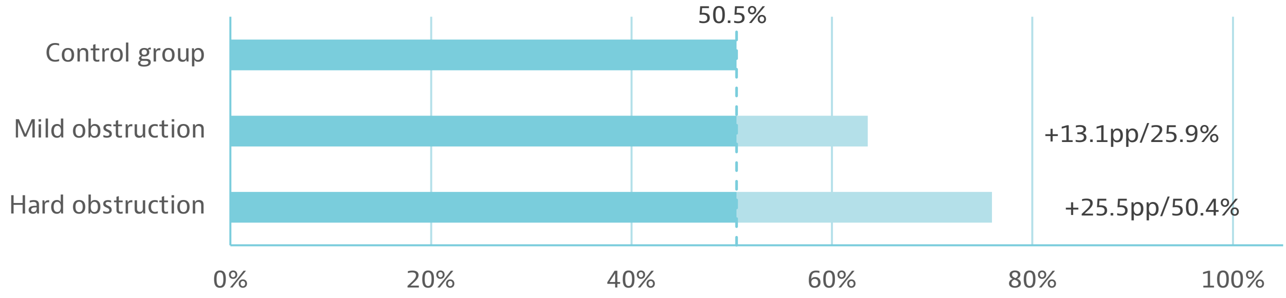
[3] OECD (2022), “Dark commercial patterns”, *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, https://doi.org/10.1787/44f5e846-en. In the report, the OECD Committee on Consumer Policy proposed a working definition of dark patterns to facilitate near-term discussion across jurisdictions: “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.”

[4] OECD (forthcoming), *Empirical study on dark commercial patterns*, OECD Publishing, Paris.

A 2024 sweep (co-ordinated screening of websites) by the International Consumer Protection and Enforcement Network (ICPEN) of 642 businesses across 26 countries determined that 75% of such businesses used at least one dark pattern in the marketing of their subscription services.[5]

A 2024 sweep by 26 privacy enforcement authorities of the Global Privacy Enforcement Network (GPEN) of 1 010 websites and apps similarly found that a majority of such websites and apps examined used privacy-intrusive dark patterns.[6] Much evidence points to the effectiveness and wide-ranging harms of such practices. For instance, online experiments in the same OECD study indicated that dark patterns could significantly, and cumulatively, influence consumers' decision-making, and lead to substantial financial impacts, disclosure of personal information, emotional distress, and time loss. All consumers, regardless of socio-demographic background, were found to be potentially vulnerable, and some, such as those of older age or using the internet infrequently, were more likely to be influenced by certain dark patterns.[7]

Figure 2. **Impact of dark patterns obstructing subscription cancellation in OECD experiments (2024)**



Note: In OECD experiments, participants were told they had been subscribed to a streaming service with a free trial. Some who tried to cancel were faced with two obstructive prompts (labelled "mild obstruction"): a trick question confirming cancellation and an offer for a discount. If they persisted, some then faced two more prompts (i.e. a total of four, labelled "hard obstruction"): one offering to set a reminder at the trial's end and another requiring a form submission to cancel. The increase in acceptance of the subscription relative to a control group resulting from the obstruction is shown, in terms of percentage point ("pp") and relative percentage differences. Results shown were statistically significant at the 0.1% level.

Source: OECD (forthcoming), *Empirical study on dark commercial patterns*, OECD Publishing, Paris.

[5] ICPEN, Dark Patterns in Subscription Services Sweep Public Report, 2024, https://icpen.org/news/1360.

[6] GPEN, GPEN Sweep 2024: Deceptive Design Patterns, 2024, https://www.privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns.

[7] OECD (forthcoming), *Empirical study on dark commercial patterns*, OECD Publishing, Paris.

OECD EMPIRICAL EVIDENCE ON DARK COMMERCIAL PATTERNS

In 2024, the OECD conducted an online survey, incorporating behavioural experiments, of over 35 000 respondents across 20 countries (18 OECD and two ASEAN member states)[8] examining the impacts of **dark patterns**. While the extent to which the results reflect reality cannot be determined definitively, the experiments were **carefully designed to elicit real consumer behaviour** within the constraints of the online survey environment.[9] In one set of experiments, respondents were told they had been signed up to a new video streaming service (which was fictitious, but framed as real) and could either proceed to set up their account (and thus accept the subscription) or cancel it. Preliminary findings relating to selected dark patterns (underlined) include:

- *False hierarchy*: 72.9% of respondents accepted the subscription when this option was made more prominent than cancelling. This compared to 47.4% for respondents for whom the options were equally prominent, implying **an increase of 25.5 percentage points (pp), or by 54% in relative terms.**
- *Additional obstruction and nagging:* 87.9% of respondents ended up accepting if, *in addition,* a series of prompts obstructed them from cancelling and pop-ups nagged them to accept. This compared to 46.7% when exposed to none of these three dark patterns (false hierarchy, obstruction, nagging), implying **an increase of 41.2pp, or by 88%.**
- *Role of consumer preferences:* Respondents who indicated they were *not interested* in getting a new subscription saw an increase in acceptance from exposure to these three dark patterns from 34.4% to 83.2% i.e. of **48.8pp, or by 142%**. This was a **greater increase** compared to those who indicated they *were interested* in getting one (53.34% to 90.08%, i.e. of 36.7pp, or by 69%).
- *Role of ability to identify dark patterns:* Respondents who identified *none* of these three dark patterns as attempts to influence their decision-making saw an increase in acceptance from exposure to them from 46.9% to 94.3%, i.e. **of 47.4pp, or by 101%**. This was a **greater increase** compared to those who identified *one or more* (46.9% to 73.9%, i.e. of 27.0pp, or by 57%).

Other experiments asked respondents to browse a simulated shopping website to select and purchase a TV as they would normally (though no actual purchase occurred). Preliminary findings include:

- *Urgency and reference pricing*: 13.1% of respondents purchased a particular high-end TV when a fake countdown timer was next to it and its price was misleadingly framed as a discount from a higher reference price. This compared to 8.7% when exposed to no such techniques, implying an **increase of 4.4pp, or by 51%**.
- *Nagging*: 24% of respondents added a wall mount to their purchase if they were nagged to do so with pop-ups. This compared to 12.8% when exposed to no pop-ups, implying an **increase of 12.2pp, or by 95%.**
- *Forced disclosure*: 58% completed the purchase even when the experiment required them to provide personal data and accept its use for marketing. This compared to 62.4% when such restrictions were not applied, implying **a *decrease* of only 4.4pp, or by 7%.**
- *Disparity between experimental and reported behaviour:* Respondents who indicated they would normally stop using websites that try to negatively influence them were **no less likely** to complete the purchase than those who did not indicate this.

These findings align with prior research and further underline the **need for robust consumer policy on dark patterns and enforcement action** against their illegal use at national and global levels.

[8] Australia, Cambodia, Canada, Colombia, Denmark, Germany, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, Sweden, Thailand, the United Kingdom and the United States.

[9] After initial survey questions, respondents were asked to navigate a simulated e-commerce website selling TVs, which they were told mimicked a real website in their country with modified brand names, and to select a TV and proceed to checkout as they would normally (though no actual purchase occurred). After checkout, they were told they were being redirected to a message from the website's partners and suddenly shown a pop-up indicating they had been subscribed to a new video streaming service (which was fictitious, but framed as real) soon to be launched in their country, with a three-month free trial. The pop-up was framed to seem believable (though respondents were later debriefed and informed the service was not real).

AI and other digital technologies can pose new and amplified risks for consumers and perpetuate consumer harms. For instance, businesses may increasingly be able to use AI and consumer data to target advertising or pricing at consumers' individual vulnerabilities, potentially triggering unwanted purchases or psychological distress.[10] AI risks exacerbating bias against certain consumer groups (defined by e.g. gender or ethnicity), whereby they are offered advertising or services on less favourable terms or excluded from offers altogether.[10] Fraudulent actors may also be able to leverage AI to carry out increasingly complex scams, including deepfakes.[10] And immersive technologies, such as virtual reality, may also provide a channel to exploit consumer immersion in unfamiliar environments, such as video games.[11]

Some consumer groups may be at particular risk of harm online. Children, including teenagers, are early adopters of digital technologies, but lack critical thinking skills to handle digital risks. These include addiction to social media, marketing blurring the lines between advertising and other content, targeted advertising and exposure to age-inappropriate products. At the same time, the above trends illustrate how online, virtually all consumers, at certain times, are harmed or at risk of harm.[10] Some scholars have accordingly characterised digital consumer vulnerability as universal or systemic.[12] While much work, including by the OECD, has contributed to understanding consumer harms online, more research is needed on emerging harms, especially given the rapid pace of technological change. This underscores the important role of the OECD and other stakeholders to develop further empirical research, incorporating behavioural insights, to expand the evidence base for policy and enforcement action.

PROTECTING CONSUMERS WITH EXISTING AND NOVEL MEASURES AND TOOLS

A strong and effective consumer policy environment enables consumers to have trust in digital markets.

Laws to combat digital consumer risks exist in many jurisdictions, in particular prohibitions on misleading, fraudulent and unfair practices, in line with the 2016 *OECD Recommendation on Consumer Protection in E-Commerce*.[13] As documented by the OECD, numerous enforcement actions have been undertaken on the basis of such laws against dark patterns and other harmful practices, such as deceptive or unfair data practices and marketing techniques and fake reviews and ratings.[14]

Consumer authorities have also upskilled in digital technologies to keep pace with their increasing business use. Some are experimenting with digital tools that could assist in detecting dark patterns, unfair contract terms, fake reviews, unsafe products and other consumer law breaches.[15] Some scholars have suggested AI could improve consumer policymaking, including through identification of consumer biases, more targeted interventions, and improved consumer research and data analysis.[16]

Nonetheless, there are concerns about whether existing laws and enforcement mechanisms are sufficiently effective and efficient to respond to the challenges. For example, there is increasing recognition that online disclosures alone may be insufficient to inform and empower consumers in

[10] OECD (2023), "Consumer vulnerability in the digital age", *OECD Digital Economy Papers*, No. 355, OECD Publishing, Paris, https://doi.org/10.1787/4d013cc5-en.

[11] Hyde, R. and P. Cartwright (2023), "Exploring Consumer Detriment in Immersive Gaming Technologies", *Journal of Consumer Policy*, Vol. 46/3, pp. 335-361, https://doi.org/10.1007/s10603-023-09544-9.

[12] Helberger, N., Sax, M., Strycharz, J. *et al.* Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability. *J Consum Policy* 45, 175–200 (2022). https://doi.org/10.1007/s10603-021-09500-5 and Riefa, C., 'Protecting Vulnerable Consumers in the Digital Single Market', (2022), 33, European Business Law Review, Issue 4, pp. 607-634, https://kluwerlawonline.com/journalarticle/European+Business+Law+Review/33.4/EULR2022028.

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

[14] OECD (2019), "Good practice guide on consumer data", OECD Digital Economy Papers, No. 290, OECD Publishing, Paris, https://dx.doi.org/10.1787/e0040128-en; OECD (2019), "Good practice guide on online advertising: Protecting consumers in e-commerce", OECD Digital Economy Papers, No. 279, OECD Publishing, Paris, https://dx.doi.org/10.1787/9678e5b1-en; OECD (2019), "Good practice guide on online consumer ratings and reviews", OECD Digital Economy Papers, No. 288, OECD Publishing, Paris, https://dx.doi.org/10.1787/0f9362cf-en.

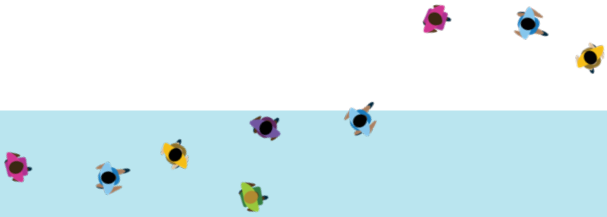
[15] Riefa, C. and L. Coll (2024), The transformative potential of Enforcement Technology (EnfTech) in Consumer Law, https://www.enftech.org/.

[16] Mills, S., S. Costa and C. Sunstein (2023), "AI, Behavioural Science, and Consumer Welfare", Journal of Consumer Policy, https://doi.org/10.1007/s10603-023-09547-6.

many situations.[17] OECD experiments in Ireland and Chile in 2019 and 2020 in particular found limited consumer ability to notice personalised pricing disclosures.[18] The complexity and opacity of digital business models also continue to challenge regulators, who may lack relevant digital technology skills or access to businesses' experimental data and algorithm outputs, and thus knowledge of the full scale of harms.

New measures are being introduced in this regard in various jurisdictions to better address ongoing and emerging digital harms. These include legal restrictions, such as on dark patterns (e.g. the EU Digital Services and Markets Acts, the UK Digital Markets, Competition and Consumers Act, Korea's updated Act on the Consumer Protection in Electronic Commerce, or India's Guidelines for Prevention and Regulation of Dark Patterns) or on AI (e.g. the EU Artificial Intelligence Act), as well as voluntary business commitments, standards and principles. Civil society also continues to play an important role, as illustrated by consumer organisations' campaigns against dark patterns, consumer tracking and loot boxes.[19]

Finally, that digital markets are borderless means international co-operation is essential. And as consumer risks online increasingly cut across policy areas, addressing them may benefit from stronger interdisciplinary co-operation.[20] For example, dark patterns, consumer tracking and manipulative personalisation can erode privacy, through deceptive data collection, and weaken competition, by hindering switching and undermining a level playing field. Accordingly, several jurisdictions have set up fora to enhance co-operation among consumer, competition, data protection and other digital regulators.[21]



QUESTIONS FOR DISCUSSION

1 What are the key opportunities and challenges for consumers online today? How do the benefits compare to the harms?

2 What are consumer policy makers and enforcers doing to tackle the challenges? What more needs to be done? How can they collaborate with counterparts in other policy areas and stakeholders to address them?

3 What further research, including by the OECD, would help better understand digital consumer issues?

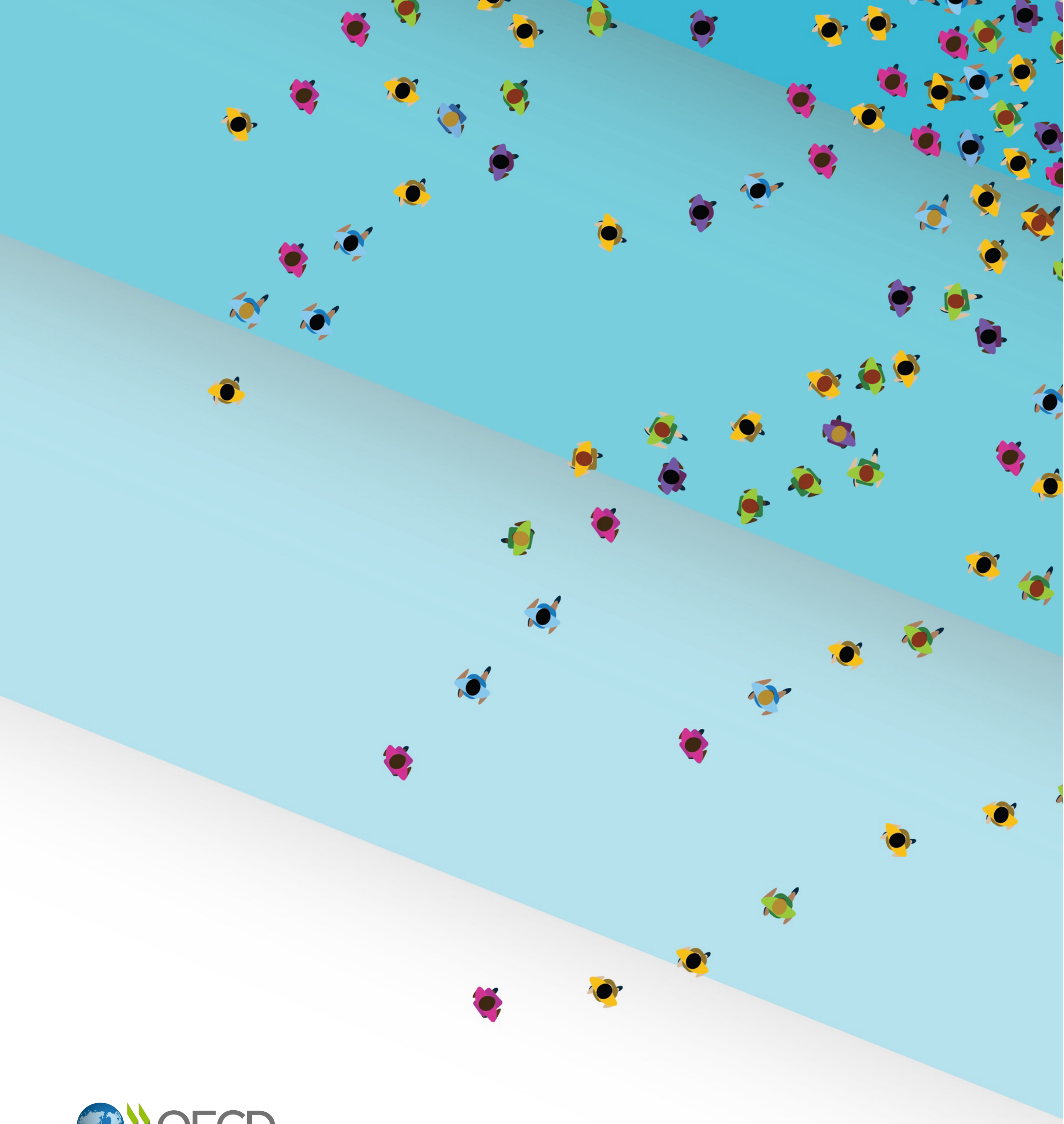
[17] OECD (2022), "Enhancing online disclosure effectiveness", OECD Digital Economy Papers, No. 335, OECD Publishing, Paris, https://doi.org/10.1787/6d7ea79c-en.

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

[19] See, for example, campaigns spearheaded by the Norwegian Consumer Council regarding dark patterns, tracking and targeted advertising, and loot boxes (defined as "mystery packages" of digital content in video games which consumers purchase with real money).

[20] OECD (2023), Applying Behavioural Insights to Consumer and Competition Policy and Enforcement - Workshop issues paper, https://one.oecd.org/document/DSTI/CP(2023)6/en/pdf.

[21] For example, the Digital Platform Regulators Forum in Australia, the Canadian Digital Regulators Forum, the Dutch Digital Regulation Cooperation Platform and the UK Digital Regulation Cooperation Forum (DRCF). The DRCF also launched the International Network for Digital Regulation Cooperation (INDRC) in June 2023 to build relationships with regulators from around the globe seeking to increase domestic co-operation in their jurisdictions.



OECD
BETTER POLICIES FOR BETTER LIVES

https://oe.cd/consumer24

ccpministerial2024@oecd.org

OECD - OECD

@OECD

@OECD_STI