

## Chapter 8

# **CONSUMER POLICY IN THE DIGITAL TRANSFORMATION**

### KEY FINDINGS

- The digital transformation is rapidly impacting the consumer marketplace, enabling purchases in multiple channels, contexts and settings. The COVID-19 crisis has accelerated these trends by leading more consumers and businesses on line.
- New technologies, such as artificial intelligence (AI) and the Internet of Things (IoT) offer greater consumer choice and personalisation, cost savings, and more convenience. At the same time, they pose new risks to safety, privacy and security, have the potential for discrimination against disadvantaged groups, and may undermine consumer trust if they are inadequately explained or if their use is not transparent. Other issues include interoperability, accountability and liability for interconnected devices, licensing and ownership, and the impact of planned obsolescence.
- Consumer policy makers are increasingly recognising the need to keep pace with technological developments and to work with counterparts in other relevant policy areas to ensure that consumers are adequately protected from unfair practices and unsafe products. They are also increasingly adopting a multidisciplinary approach to identify and address consumer policy issues, incorporating learnings from economics, psychology, cognitive and social sciences and empirically tested results in order to understand and guide consumer behaviour.

### Introduction

This chapter outlines some of the key technological trends and developments affecting consumer policy in the digital transformation. It provides an overview of consumer benefits and risks associated with new technologies, including the Internet of Things and artificial intelligence. It discusses how these new technologies can, or could, be employed to enhance consumer protection and product safety. It also examines how consumer biases impact consumer behaviour online. It highlights policy makers' growing recognition of the need to consider behavioural insights in designing more effective consumer policies. It reflects on how policies can enhance consumer trust and thereby maximise the development and adoption of new technologies.

### Technological trends and developments

E-commerce is in transition. Traditional e-commerce “storefronts” and marketplaces are moving to environments that enable consumers to make purchases in multiple channels, contexts and settings. These range from social media marketplaces to voice-activated transactions. In addition, digital and mobile payment is providing consumers with greater convenience and new types of consumer-facing products fuelled by consumer data and incorporating new technologies continue to emerge.

The COVID-19 crisis has accelerated these trends, and associated challenges, leading more consumers to access goods and services on line. This has caused many businesses to rapidly adopt a digital model in response (OECD, 2020<sub>[1]</sub>). Many of these online shifts will likely remain once the health crisis dissipates, as consumers and businesses grow used to the convenience of online channels.

### Benefits and risks of new technologies

Businesses are increasingly using new technologies in a range of innovative consumer products. These developments could benefit consumers by offering the following:

- New and innovative goods and services, providing greater choice for consumers. For example, many IoT products bring entirely new services and functionalities (OECD, 2018<sub>[2]</sub>; 2018<sub>[3]</sub>).
- Cost savings, including reduced transaction and search costs.
- Greater personalisation, building on the wealth of consumer data collected online, to constantly offer more tailored products and services to consumers (OECD, 2019<sub>[4]</sub>; Consumers International, 2019<sub>[5]</sub>).

- Convenience, customisation and remote control, especially for a number of IoT products in the smart home (OECD, 2018<sub>[2]</sub>; 2018<sub>[3]</sub>).
- Support for biased-free decisions. Products powered by AI, such as digital assistants, can theoretically make suggestions free from consumers' behavioural biases (OECD, 2019<sub>[4]</sub>).

However, a number of new consumer risks are associated with new technologies:

- **Transparency and disclosure.** Adequate disclosures and transparency are important to building consumer trust and effective competition in the digital transformation (OECD, 2010<sub>[6]</sub>). Lack of transparency and overly complex, legalistic or otherwise inadequate disclosures, especially about how consumer data are collected, used and shared, appears to be common (OECD, 2018<sub>[3]</sub>; OECD, 2017<sub>[7]</sub>; Consumers International and The Internet Society, 2019<sub>[8]</sub>; OECD, 2019<sub>[9]</sub>). A similar lack of transparency may exist in regard to when and how AI is used in consumer goods and services. Consumers may also be kept in the dark about planned obsolescence of products relying on aftermarket support. This may create unexpected costs for consumers who need to replace devices.
- **Discrimination and choice.** More collection and use of consumer data, coupled with the use of AI could lead businesses to discriminate against consumers. This could manifest in pricing, or in presentation of offers and information (Richmond, 2019<sub>[10]</sub>; OECD, 2019<sub>[11]</sub>). It also presents the risk of unfair or discriminatory outcomes or perpetuation of socio-economic disparities (Smith, 8 April 2020<sub>[12]</sub>). This may involve discrimination against already disadvantaged groups of consumers, such as women and ethnic minorities.
- **Privacy and security.** Personal data are increasingly collected and used. Meanwhile, IoT products, such as digital assistants, health tracking devices and “smart home” appliances, continue to proliferate and are increasingly interconnected. This can increase threats to privacy and security (OECD, 2018<sub>[2]</sub>; 2018<sub>[3]</sub>).
- **Interoperability.** Interoperability is key to ensuring that different systems and devices can work together. Some restrictions on interoperability may spur innovation, and improve privacy and security. However, a degree of interoperability is needed to avoid “lock-in” and support choice and competition (OECD, 2018<sub>[3]</sub>).
- **Accountability.** Consumers may struggle to understand who is accountable and liable for interconnected IoT devices and ecosystems. It may not be clear to consumers which part of the ecosystem (or service support) caused the issue or fault with their device (OECD, 2018<sub>[2]</sub>; 2018<sub>[3]</sub>). Accountability is also a key issue for AI. The OECD *Recommendation of the Council on Artificial Intelligence* requires that AI actors be accountable for the proper functioning of their systems, and for respect of the principles in the Recommendation (OECD, 2019<sub>[13]</sub>).
- **Ownership.** When a consumer buys an IoT device (or a product using AI), they buy the device itself (the hardware), and a licence granting the right to use the software. The licensing conditions may limit the degree to which a product may be repaired, modified or resold, undermining traditional assumptions regarding product ownership (OECD, 2018<sub>[3]</sub>).
- **Need for aftermarket support.** Most IoT devices require software support and Internet connection to work effectively. If a manufacturer withdraws support, a device may not function as intended. Further, a lack of support could make a device vulnerable to security breaches. This could result in risks to privacy, security or safety (OECD, 2018<sub>[3]</sub>).

### Enhancing consumer protection with new technologies

New technologies provide new benefits and risks for consumers. At the same time, they offer new opportunities for policy makers, enforcement agencies and civil society in tracking and identifying emerging consumer issues and violations of the law. They also offer new ways of potentially protecting consumers from certain threats, including unsafe products.

AI could help consumer protection authorities identify “dark patterns” and fake consumer ratings and reviews on line. In addition, it could be used to scan online ratings and reviews, as well as comments on social media and other websites, such as marketplaces. This could identify recurring themes and issues that represent consumer problems.

A recent study by Mathur et al. (Mathur et al., 2019<sub>[14]</sub>) of Princeton University's Center for Information Technology used AI to identify “dark patterns” in a survey of 53 000 product pages from 11 000 shopping websites. Dark patterns are tactics employed by businesses in websites and apps to coerce, steer, or

deceive consumers into making unintended and potentially harmful decisions (Mathur et al., 2019<sup>[14]</sup>; Dark Patterns, n.d.<sup>[15]</sup>). Dark patterns may take various forms. Examples include using opt-out check boxes to sneak unwanted items into online shopping carts, subscriptions that are easy to start but difficult to cancel or using language to shame a consumer into opting into something (Dark Patterns, n.d.<sup>[15]</sup>). The technology and methodology used by Mathur et al. could presumably be adapted and used by consumer agencies or other interested parties to scan and identify certain forms of concerning conduct used by online businesses.

The identification of fake reviews, which may also constitute a dark pattern, is another area in which there could be a role for AI or related technologies. Consumers are indeed increasingly relying on online ratings and reviews despite concerns about the truthfulness of some online ratings and reviews (Ofcom, 2017<sup>[16]</sup>; Lester, 2019<sup>[17]</sup>). In the OECD's survey on consumer trust in peer-platform marketplaces, 73% of consumers identified the ability to see ratings and reviews as an important trust mechanism (OECD, 2017<sup>[7]</sup>). Methodologies that could help identify fake reviews would be useful in improving the overall reliability and trustworthiness of online ratings and reviews, which is important to consumer trust in e-commerce.

Such uses of AI for enforcement and policymaking purposes, however, could raise legal, ethical, or other challenges for consumer authorities, and there may be, for example, limitations imposed by data protection laws. Consumer authorities are beginning to consider how to deal with these and other issues (i.e. privacy and data security) including through exchanges in international enforcement networks.

New technologies also underpin development of a range of new goods and services to protect consumers on line. Some envision a world where algorithms can do everything for the consumer – from identifying a need to selecting the best deal to ordering and paying for a product or service on line (Gal and Elkin-Koren, 2017<sup>[18]</sup>). The development of algorithmic consumers is in its infancy, but online price comparison sites based on algorithms are well established. Other new consumer tools are also being developed, including tools to assist consumers in identifying potentially problematic terms and conditions in end-user license agreements.

### Enhancing consumer product safety with new technologies

New technologies, such as the IoT and AI, may also be used in innovative ways to enhance consumer product safety.

### The Internet of Things

The IoT includes all devices and objects whose state can be altered via the Internet, with or without the active involvement of individuals (OECD, 2018<sup>[19]</sup>). While connected objects may require the involvement of devices considered part of the “traditional Internet”, this definition excludes laptops, tablets and smartphones already accounted for in current OECD broadband metrics. The range and number of devices incorporating IoT technology is growing rapidly across OECD countries (OECD, 2018<sup>[2]</sup>). It increasingly includes many non-traditional devices (including household locks, cameras, and automobiles) connected *en masse* in order to deliver seamlessly connected experiences in households and businesses.

Manufacturers may be able to identify and remedy product safety issues in IoT products more efficiently due to their Internet connection. Some examples follow:

- Tracking and tracing products in the market may help identify affected consumers in the context of a product safety recall.
- Remote monitoring may enable quicker detection of safety defects in products. In some cases, defects can be remedied via remote software patches. This would avoid the need for recalls and reduce consumer inconvenience and recall fatigue.
- Consumers could receive real-time alerts of product recalls via their display screen or audio capability.
- Manufacturers could power down or switch off recalled products remotely while the products remain in the consumers' hands.

A recent example of the capabilities of IoT technology to enhance product safety occurred in the recall by Samsung of 4.6 million Galaxy Note7 phones. In 2016, Samsung conducted a software update that

reduced the battery capacity of the phones that were still in consumers' hands down to 0%. It also sent more than 23 million recall alerts and push notifications to its customers on their affected phones (OECD, 2018<sub>[20]</sub>).

Despite these benefits, the IoT market may also bring new safety risks due to the increasing complexity of products and the growing and competitive environment that has pushed businesses to get IoT products to market as quickly and inexpensively as possible. An IoT product may be unsafe when entering the market due to a latent software defect, but may also become unsafe once placed on the market following a software update. The integrity and quality of input data may also impact the safety of those IoT products that rely on data inputs. For example, an automated vehicle may rely on input data to detect safety and performance issues and to schedule maintenance. IoT products may also present a safety risk if they lose Internet connectivity during use. Safety risks may also emerge if consumers continue to use IoT devices that are considered “end-of-life” and are no longer monitored or serviced by the manufacturer.

In addition, there is growing recognition of the convergence between product safety, privacy and digital security in the IoT. Given that all software contains vulnerabilities, malicious actors could exploit or hack IoT devices. For example, they may use IoT devices to track an individual's location for surreptitious surveillance.

Concerns with consumer security and safety are growing, and many private-sector initiatives are underway to keep up with IoT safety and security challenges. The dynamic risk environment also requires proactive engagement from consumers and governments to address cross-cutting cyber resilience challenges as government regulatory efforts in this space are still nascent.

Indeed, as the IoT continues to grow and permeate our lives, complex consumer policy issues continue to emerge that may raise competing interests. For example, the ability for manufacturers to remotely power down products already in the market in order to address hardware/software issues may provide obvious benefits to product safety, but has also been criticised given the impact on a product's performance and value.

### Artificial intelligence

AI has the potential to improve consumer product safety in the near future. AI-embedded products with the capabilities to learn based on the collection of consumer data may be designed to adapt to consumer behaviour, within the limits of applicable data protection laws. In theory, such products could detect consumer behaviour patterns. For example, they may identify an unintended use of the product, one not anticipated by the designer that may create a safety risk. In such cases, the product may adapt its own performance to reduce or eliminate the risk. AI may also enable products to predict the need for servicing or maintenance based on their use over time.

AI also has other uses in post-market product safety surveillance of both connected and unconnected products. AI may help identify safety risks by analysing usage data collected from products across complex and global supply chains, enabling early detection of product defects and earlier interventions in the form of product recalls and improvements to safety features if the product is still in production. AI may also interrogate data collected from other sources, such as product review sites, to identify new and emerging product safety risks. Some online marketplaces are already using AI to block or remove banned and recalled products from their sites by identifying keywords used in product descriptions.

On the other hand, AI may also bring new risks of manipulation of consumer preferences or failure of the AI-embedded product through biases and system vulnerabilities. That is why an AI system's robustness, security and safety must be ensured not only at the time of creation or launching of the system, but over its entire life cycle (OECD, 2019<sub>[13]</sub>).

### Key challenges for governments

Governments need to consider how to adapt, change, and implement consumer policy in this age of rapid technological progress. While consumer policy is generally broad enough to cover new technologies and business models, governments should ensure that there are no gaps in government

policy and competency that leave consumers exposed (OECD, 2019<sup>[21]</sup>). Governments have a key role in ensuring that new technologies are being used in a human-centric, ethical, and sustainable way to maintain consumer trust.

Another key challenge for governments is to ensure they have the necessary technical expertise to understand these emerging issues. This will allow them to make and enforce policy effectively. In addition, many risks span several areas, including data protection, privacy, consumer protection, competition, intellectual property and security. Therefore, consumer authorities need to co-operate and co-ordinate with their counterparts in other relevant disciplines. Furthermore, the global nature of the digital transformation implies that governments increasingly need to co-operate across borders. They should enhance their authority to do so, including by implementing the co-operation provisions of the 2016 *Recommendation of the Council on Consumer Protection in E-commerce* (hereafter “E-commerce Recommendation”) (OECD, 2016<sup>[22]</sup>) and the 2003 *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders* (OECD, 2019<sup>[21]</sup>).

When it comes to risks associated with new technologies, there is scope for consumer policy to consider the vulnerabilities of different groups of consumers, including the elderly and children, to target protections and awareness accordingly. In this way, they can ensure the benefits of new technologies are shared across society. Some consumer groups, such as the elderly, may be more prone to online scams (ACCC, 2020<sup>[23]</sup>) and data protection and privacy concerns may be more sensitive when it comes to IoT products used by, and aimed at, children who may be less aware of the risks (OECD, 2018<sup>[2]</sup>).

In addition, the COVID-19 crisis shows that policy makers should also consider whether large-scale events, such as pandemic or natural disaster, might render wider groups of consumers vulnerable to online commercial exploitation. For example, the pandemic has made many mainstream groups of consumers more vulnerable. Job and financial losses, along with fear and anxiety regarding the virus, may open consumers to risk from exploitative practices on line, such as price gouging of essential or in-demand products (OECD, 2020<sup>[1]</sup>).

Encouraging businesses and industry associations, as well as consumer and other civil society organisations, to provide input into policies regarding the incorporation of new technologies in consumer products is important. This will help ensure that new products benefit consumers without harming them economically, compromising the privacy or security of their personal information, or otherwise putting them at risk.

### Using behavioural insights to address consumer policy challenges in the digital transformation

Consumer policy has often been justified as a response to market failures. For example, requirements around information provision and protections against false or misleading information are intended, among other things, to address market failures associated with imperfect and/or asymmetric information. These objectives remain paramount, particularly in the face of digital transformation. However, improved understanding of consumer behaviour through behavioural insights and empirical studies have added new dimension to, and justifications for, consumer policy.

Behavioural insights is a multidisciplinary approach to policy making. It combines insights from psychology, cognitive science, economics and social science with empirically tested results to discover how humans actually make choices. To that end, it incorporates methodologies from behavioural economics, including psychological insights into the study of economic problems. It also embraces information economics, which focuses on the quality, quantity, costs and accessibility of information available to consumers.

Behavioural insights have shown that consumers can be subject to biases that might limit the effectiveness of some consumer policy. This is especially the case for information disclosures, pricing information and informed consent (OECD, 2018<sup>[24]</sup>; 2017<sup>[25]</sup>). Further, behavioural insights can highlight how certain businesses can provoke consumers to act in ways that may conflict with their own best interests. Box 8.1 outlines some key behavioural biases relevant to consumer policy.

Understanding consumers and policy impacts in this way provides the depth of insight needed for the increasingly complex policy decisions required in the digital transformation. Many behavioural insights

show how consumers form trust relationships with industry, specific brands and governments. These, in turn, provide tools for policy makers to understand behavioural and social needs.

The COVID-19 crisis has underscored the importance of incorporating behavioural insights into consumer policy. The crisis has undeniably exacerbated a number of key consumer behavioural biases (OECD, 2020<sub>[1]</sub>). For example, the panic buying in many countries during the earlier stages of the crisis highlights the power of a number of the common behavioural biases outlined in Box 8.1. Loss aversion is particularly important, as well as social and cultural norms as the actions of peers often guide consumer behaviour.

**Box 8.1. Behavioural biases relevant to consumer policy and consumer product safety**

**Information overload.** When faced with complex products or a bewildering array of choices, consumers may ignore possible choices or choose not to choose. Consumers may also rely on simple “rules of thumb” or “heuristics”.

**Default and status quo effect.** Presenting one choice as a default option can induce consumers to choose that option. The power of the default setting relates to the status quo effect, where consumers have a strong tendency not to change.

**Endowment effect.** Consumers often demand much more to give up an object than they would be willing to pay to acquire it: consumers value a product more highly when it becomes part of their endowment. This is because consumers tend to be loss averse.

**Framing.** The presentation of information affects how consumers perceive and interpret it. Presenting an option in a certain way may induce consumers to evaluate the choice from a particular reference point.

**Anchoring.** Consumers can “anchor” decisions around information they think is most important. This means consumers may not change their minds about the value of an offer, even when they receive additional information.

**Priming effect.** When consumers are repeatedly exposed to something, for example, through publicity, certain attributes of the product can “prime” the consumer towards a decision to purchase. Priming can influence preferences by making certain attributes appear more important than they should be.

**Overconfidence.** Consumers tend to think they are more likely to experience an outcome from some action that is better than the average expected outcome. For example, most drivers think they are safer than the average driver.

**Hyperbolic discounting and myopia.** Consumers tend to treat the present with much more importance than the future. This explains outcomes such as low voluntary retirement savings.

**Time-inconsistency.** Consumers may make choices inconsistent across time due to conflicts between short-term urges and long-term interests.

**Social and cultural norms.** Consumers are often guided by the values, actions and expectations of a particular society or group. For example, when people are made aware of what others are doing, it can reinforce individuals’ underlying motivations.

Source: Adapted from OECD (2018<sub>[24]</sub>), “Improving online disclosures with behavioural insights”, <https://dx.doi.org/10.1787/39026ff4-en>.

### Improving online disclosures

There are a number of ways in which consumer agencies and international organisations, such as the OECD, have been incorporating behavioural insights into consumer policymaking, however a key area in which this is occurring is in relation to online disclosures. For example, in 2018, the OECD published a report on improving online disclosures with behavioural insights (OECD, 2018<sub>[24]</sub>). The purpose of

the report was to assess ways in which consumers' behavioural biases may impact the effectiveness of online disclosures, and to suggest ways in which to develop online information disclosures that incorporate behavioural insights. The Netherlands Authority for Consumers and Markets also calls for greater transparency in online disclosures in its recently released guidelines on the boundaries of online persuasion, which incorporate learnings from behavioural insights (ACM, 2019<sub>[26]</sub>).

Policy makers have long understood the importance of helping consumers overcome imperfect and asymmetric information (OECD, 2016<sub>[22]</sub>). As the 2016 E-commerce Recommendation underscores,

*[o]nline disclosures should be clear, accurate, easily accessible and conspicuous so that consumers have information sufficient to make an informed decision regarding a transaction. Such disclosures should be made in plain and easy-to-understand language, at a relevant time, and in a manner that enables consumers to retain a complete, accurate and durable record of such information. (Principle 21)*

Relevant information can include background on the seller, the goods and services on offer, and the transaction itself, including payment methods, privacy policies and available dispute resolution and redress options. It can be provided in different ways and at various times in a transaction. This includes through advertising and marketing, contractual terms and conditions, and legally required notices. In addition to disclosure requirements, many jurisdictions have prohibitions on the provision of false and misleading information to consumers (OECD, 2016<sub>[22]</sub>).

While information disclosure requirements remain a key policy tool for empowering consumers on line, findings from behavioural insights raise concerns about their effectiveness in some circumstances.

First, consumers can be subject to information overload. When confronted with complex products or a large range of choices, consumers can struggle to decide. Ultimately, information overload can lead to consumer detriment if it makes them defer a decision or make the wrong choice based on relatively simple "rules of thumb".

Numerous studies have found that consumers are particularly prone to information overload when shopping on line, such as Benartzi and Lehrer (2017<sub>[27]</sub>), and Office of Fair Trading (United Kingdom) (2007<sub>[28]</sub>). Information overload is one reason why few consumers read online terms and conditions (T&Cs) in full. Estimates of readership vary dramatically, suggesting between 0.2% and 77.9% of consumers read at least some online T&Cs (European Commission, 2016<sub>[29]</sub>; Stark and Choplin, 2009<sub>[30]</sub>; Bakos, Marotta-Wurgler and Trossen, 2014<sub>[31]</sub>; OECD, 2017<sub>[7]</sub>). Online readership depends on the way T&Cs are presented, the product they relate to and how readership is measured. Further, businesses can potentially take advantage of information overload by making their goods, services or prices more complex than required. Bar-Gill (2012<sub>[32]</sub>) has raised concerns about this in the credit card, mortgage and mobile phone markets.

Second, framing and anchoring effects can influence a consumer's ability to understand online information disclosures.

Through framing, consumers are influenced by both the content and presentation of the information provided (Tversky and Kahneman, 1981<sub>[33]</sub>). The visual presentation of websites and mobile apps, timing of disclosure, text font and size, and use of colour, images and video, all affect how consumers absorb information. This has been demonstrated in a number of studies (FTC, 2013<sub>[34]</sub>; 2017<sub>[35]</sub>; 2016<sub>[36]</sub>). For example, the Behavioural Insights Team in the United Kingdom suggested that framing can improve both consumer understanding of, and interaction with, T&Cs and privacy policies (Box 8.2).

Anchoring occurs when consumers weigh one piece of information too heavily when making a decision, often at the expense of other information (Tversky and Kahneman, 1981<sub>[33]</sub>). This can mean that consumers do not evaluate the entire offer properly, even when additional information is provided, which can lead to consumer detriment.

Third, in some markets, the information required to make sound decisions overwhelms many consumers. In many cases, comparator websites and other intermediary services have emerged to address this problem. However, consumers often require complex information (e.g. about their usage) to take advantage of these services. Policies that enable more complex information to be accessed in a machine-readable format could allow consumers to make better use of services offered by intermediaries.



**Box 8.2. Improving terms and conditions with behavioural insights**

The United Kingdom's Department of Business, Energy and Industrial Strategy commissioned the Behavioural Insights Team (BIT) to create a best practice guide for businesses on improving consumer understanding of contractual terms and privacy policies. Based on a literature review and behavioural experiments, the guide indicates that a small proportion of consumers properly read or understand T&Cs when buying on line. To improve consumer understanding, it recommends that businesses:

- Use a question and answer format to present the key terms.
- Summarise key terms and illustrate them with explanatory icons, to reduce the amount of information given in one go.
- Use a scrollable text box instead of requiring consumers to click through to view T&Cs.
- Provide information in short chunks at the right time.
- Use comics and illustrations to explain step-by-step actions and processes.

In addition, BIT suggested that businesses can increase the chance of consumers opening T&Cs and/or privacy policies by:

- telling them how long a policy normally takes to read
- announcing their last chance to read information before deciding.

Source: Bohn (2019<sup>[37]</sup>), "The T-Mobile-Sprint merger could mean the end of the physical SIM card", <https://www.theverge.com/2019/7/26/8931784/t-mobile-sprint-merger-esim-justice-department-requirement-sim-card>.

**Encouraging meaningful consumer consent**

In one key lesson from behavioural insights, consumers tend to stick with the default option (or status quo) rather than actively choosing another alternative or opting-out of the default (Kahneman et al., 1991<sup>[38]</sup>; Sunstein, 2013<sup>[39]</sup>). This can potentially lead to consumer harm if they stick with a default although it is not in their best interests. The issue of default settings has been widely researched across a range of areas including savings plans (Carroll et al., 2009<sup>[40]</sup>), organ donation (Johnson and Goldstein, 2004<sup>[41]</sup>), retirement plans (Samuelson and Zeckhauser, 1988<sup>[42]</sup>), insurance (Johnson et al., 1993<sup>[43]</sup>) and privacy (Johnson, Bellman and Lohse, 2002<sup>[44]</sup>).

In a consumer context, default settings can undermine meaningful consent. In negative option marketing, for example, a customer's failure to take affirmative action to reject or cancel an agreement is taken as assent. Consumers can thus unwittingly opt in for additional goods or services with associated fees or charges (OECD, 2019<sup>[4]</sup>). This is because consumers tend to ignore pre-checked boxes, especially on line (FTC, 2009<sup>[45]</sup>). Pre-checked boxes or other default settings can automatically sign consumers up for additional goods or services, financial commitments, disclosure of personal data or marketing material. A significant proportion of consumers will likely fail to uncheck these options or change the default despite not actually wanting them or agreeing with them. This has a great potential to result in consumer detriment.

In recognition of this, the European Union has banned pre-ticked boxes on line under its Consumer Rights Directive (2011<sup>[46]</sup>). The European Commission did not undertake a specific trial before banning pre-checked boxes since "available evidence was considered compelling enough to support the policy initiative" (Sousa Lourenço et al., 2016, p. 16<sup>[47]</sup>). Similarly, British consumers are not bound by charges for any goods that are sold by way of pre-ticked boxes (The Consumer Contracts [Information, Cancellation and Additional Charges] Regulations 2013). Similarly, under the Restore Online Shoppers' Confidence Act in the United States, enacted in 2010, businesses must obtain a consumer's express consent before charging for any goods or services purchased on line. In addition, for online goods or services sold through a negative option feature, businesses must also provide consumers with details of the transaction and a simple means to opt-out of any reoccurring charges. Such negative option features include a continuity plan, "free trial" conversion or automatic renewal programme.

Similarly, automatic renewal of contracts, which preys on consumers' status quo biases, have been viewed unfavourably by a number of consumer agencies across the OECD. In many cases, they have been found to be unfair practices, and hence, unlawful (Kovač and Vandenberghe, 2015<sup>[48]</sup>). Businesses should ensure they receive meaningful consent from consumers. In this regard, pre-checked boxes and negative option marketing strategies are insufficient.

Default and status quo biases may also lead consumers to disclose and share more personal information than they would otherwise choose. Default privacy settings lead to a high level of disclosure and sharing. Therefore, consumers could disclose and share more personal information than they would otherwise choose, had they actively considered the choice (Calo, 2014<sup>[49]</sup>). Conversely, default privacy settings that are more protective of consumers may be an effective way to improve their privacy. Meaningful consent provides a "first step" to the consumer experience. A consumer can consent to the myriad of pricing practices listed below. However, they must feel empowered to have subjected themselves to this practice willingly, with a reasonable understanding of the benefits and risks therein. In this way, meaningful consent is closely related to consumer trust.

### Better understanding the impact of personalised pricing

Personalised pricing is another issue that relates to online disclosures and that is attracting increasing attention from policy makers across the areas of consumer and competition policy (OECD, 2018<sup>[50]</sup>). For example, in October 2019, an EU Directive was adopted on the better enforcement and modernisation of EU consumer protection rules providing for enhanced transparency in the use of personalised pricing in online transactions (European Commission, 2019<sup>[51]</sup>)

Personalised pricing involves the use of personal data to charge consumers different prices based on their personal characteristics (OECD, 2018<sup>[50]</sup>). It can be distinguished from dynamic pricing, where prices may fluctuate at different times due to supply and demand differences, or personalised ranking, whereby following a transaction a consumer may be presented with recommended products that were purchased by other consumers who also purchased that other product. It has been defined as

*[...] the practice where businesses may use information that is observed, volunteered, inferred, or collected about individuals' conduct or characteristics, to set different prices to different consumers (whether on an individual or group basis), based on what the business thinks they are willing to pay. (CMA, 2018, p. 36<sup>[52]</sup>)*

While, to date, there is no systematic evidence of personalised pricing, growing use of data analytics and pricing algorithms mean that businesses have the ability to engage in personalised prices, especially in e-commerce. Despite this technological feasibility, consumer discomfort with personalised pricing may be the reason why there appear to be so few documented cases of personalised pricing (OECD, 2018<sup>[53]</sup>).

From a policy perspective, the impacts of personal pricing are ambiguous. On the one hand, from a competition perspective, personalised pricing could in some cases enhance competition, increasing both total and consumer welfare. In particular, personalised pricing may intensify competition by allowing firms to target prices to poach their rivals' customers (OECD, 2018<sup>[50]</sup>). Personalised pricing has the potential to improve consumer welfare through allocative efficiency and benefit low-end consumers who would otherwise be underserved by the market. On the other hand, in some circumstances, personalised pricing can lead to a loss in total consumer welfare, where businesses benefit at the expense of consumers. Even where consumers as a whole are not worse off, some consumers may benefit at the expense of others.

Notwithstanding this, if personalised pricing is undertaken using non-transparent or deceptive means, or otherwise violates privacy, data protection, or anti-discrimination laws, it could reduce market trust and create a perception of unfairness, potentially dampening consumer participation in digital markets (OECD, 2018<sup>[50]</sup>). Given this, the OECD has developed work to understand the impact of disclosures about online personalised pricing on consumer awareness and behaviour. To test this, the CCP engaged the Behavioural Research Unit of the Economic and Social Research Institute (ESRI) to undertake a laboratory experiment in their offices in Dublin, Ireland. The purpose of the experiment was to test: i) whether disclosure enables consumers to identify and comprehend personalised pricing; and ii) what impact disclosure has on consumer behaviour and decision making. Additionally, a survey was added, among other things, to learn more about consumers' fairness perception of personalised pricing. In March 2020, ESRI repeated the experiment and survey in Chile to test for country differences.

According to the survey results, most consumers in Ireland did not think online personalised pricing should be allowed, with perceived fairness affected by whether a discount or a price hike was involved. The preliminary results for Chile seem to support this result on average, though the acceptance of personalised pricing was slightly higher. However, results from the experiment in both countries suggest that disclosures about personalised pricing do not have a significant effect on consumers' practical purchase choices. Moreover, a minority of participants recalled seeing a disclosure (amounting in Ireland to between 6% and 21% for the weak disclosure and 22% to 38% for the strong disclosure, and in Chile, between 0% and 7% and 4% to 10%, respectively). These results raise important questions not only about the behavioural response of consumers to personalised pricing in practice, but also the limitations of even clear and salient disclosures as a consumer protection tool. Further experiments with more dynamic forms of disclosure (e.g. with different timing, placement, colours, or wording) and even more explicit information about personalisation of prices and pricing strategies may be beneficial. This work highlights the question of how to increase disclosure effectiveness more generally, an issue highly relevant for consumer behavioural work overall.

### Better understanding the impact of online advertising

Advertising is always seeking to influence consumers into making purchases (OECD, 2019<sup>[54]</sup>). To that end, it has long employed psychologists and other behavioural scientists (Packard, 1957<sup>[55]</sup>; OECD, 2019<sup>[4]</sup>). However, digital technologies and web design open up new possibilities to control and manipulate consumers on an unprecedented scale.

Developments in AI and machine learning, coupled with online data collection, have enabled cost-effective, precision-targeted (and retargeted) advertising at an unprecedented scale (OECD, 2019<sup>[4]</sup>). This has been called online behavioural advertising, online profiling and behavioural targeting. Such advertising uses information such as age, gender, location, education level, interests, online shopping behaviour and search history. Complementary technologies track user interaction with online ads to determine the effectiveness of advertising campaigns. They also provide the infrastructure for advertising payments to be tied to specific user outcomes such as “clicks”, webpage visits or purchases (OECD, 2019<sup>[4]</sup>).

These developments can provide both benefits and risks for consumers (OECD, 2019<sup>[4]</sup>). Benefits include more targeted, relevant and timely ads. These could reduce search costs and improve awareness of relevant products and identification of, and access to, better deals. Online advertising also funds a range of nominally free online services, including search services, social networking services and digital news outlets. Risks include longstanding concerns around advertising's potential to mislead or deceive, as well as new concerns. Emerging issues include i) consumers' (in)ability to identify some forms of online advertising; ii) impacts on consumer trust on line; iii) the ability for online advertising to prey on consumer biases and vulnerabilities; iv) threats from “malvertising”; and v) threats associated with increased data collection (OECD, 2019<sup>[4]</sup>).

Anchoring and framing effects may inhibit a consumer's ability to identify online advertising. In particular, native and user-generated advertising can be difficult to identify. If consumers do not identify such content as advertising, they may give it greater weight than if they had known. Anchoring could also lead consumers to make mistakes in valuing an offer or in comparing offers. Personalised advertising can anchor or frame an advertisement to highlight characteristics of the product or service valued by the consumer, while downplaying others. This could also raise issues, especially if it misleads or deceives consumers.

Many jurisdictions have long had safeguards against risks associated with advertising and marketing. The 2016 E-commerce Recommendation, for example, includes provisions relating to advertising and marketing. These provisions ensure that consumers understand when they are dealing with online advertising and that such advertising is not false or misleading.

The ability of online advertising to exploit consumer biases at scale is a new issue. It arises from the increased ability of businesses to engage in targeted online advertising. Consumer decisions may be more prone to manipulation through online advertising than through other forms (Richmond, 2019<sup>[10]</sup>). Some commentators have also raised concerns about online advertisers using “persuasion profiling” to use the social norms that resonate best with a particular consumer. This could be used to target a

consumer in real time based on a consumer's habits, location and general vulnerabilities (Calo, 2014<sup>[49]</sup>). Using this form of targeting to mislead consumers could potentially harm them.

### *Designing more effective product recall notices*

The number of product recalls is growing worldwide (OECD, 2018<sup>[56]</sup>). Accordingly, the need to communicate product recalls effectively to consumers has never been more important. In recent years, the OECD has examined how consumer biases inhibit recall effectiveness and how behavioural insights can help inform the practical implementation of recalls to improve their effectiveness (OECD, 2018<sup>[56]</sup>).

According to a number of studies, several factors inhibit the effectiveness of product recalls. For example, consumers often do not spend time reading product recall notices. Even when they do, they either do not understand them or simply choose not to react. In some cases, consumers' lack of response has resulted in serious injury and death. These outcomes can take place years after a recall and despite repeated attempts from businesses and authorities to alert consumers about the need to return their product (OECD, 2018<sup>[56]</sup>).

Consumers tend to be confident that products sold in physical stores and online shops are safe (Wood, 2016<sup>[57]</sup>). As a result, they generally do not read, or fail to act upon, product safety instructions (CPSC, 2003<sup>[58]</sup>). Several other factors may explain consumer inaction to recall notices. These include the combination of consumer biases and the low value and/or short lifespan of a particular product; the level of severity of the hazard; remedies offered to consumers; and ways in which consumers are contacted.

Better understanding of consumer biases can help businesses and governments develop more effective communication strategies to increase consumer engagement with product recalls. Use of multiple channels to communicate a recall may overcome some consumer biases. Multiple channels should include both direct communication methods (email, letter, phone, SMS, in-person visits) as well as broader advertising campaigns (posters, television, radio, websites, social media, influencers).

The content of recall communications should also incorporate learnings from behavioural insights. To motivate consumer action, recall communications should give consumers a sense of urgency and severity. They should use well-understood words such as "Urgent" and "Danger". They should also show pictures of the risk. As well, they should avoid technical jargon and misleading phrases about the severity of the risk such as "voluntary recall". Recall communications may also include behavioural "nudges" to motivate consumer reaction such as the following:

- **References to social norms.** Highlighting that most people engage in or approve the same behaviour.
- **Reciprocity.** Providing consumers with an unexpected gift to induce compliance with the notice (in addition to the remedy for the unsafe product).
- **Personalisation.** Attracting attention by using the recipient's name in the communication.
- **Simplification.** Making the recall easy to understand and allowing consumers a simple option for following up on the recall.

The OECD is developing policy guidance for governments and businesses on maximising recall effectiveness. This work, which will draw on learnings from behavioural insights, was expected to be released by the end of 2020.

Consumers around the globe are experiencing rapid change due to the digital transformation, especially with the arrival of AI and the IoT. These, and other new technologies, are making possible a range of innovative goods and services, even as they radically transform existing ones. The COVID-19 crisis has heavily accelerated consumer adoption of new technologies, e-commerce and online models. These shifts will likely remain even after it is safe for consumers to engage fully with the brick-and-mortar experience again.

While these new technologies provide consumers a wealth of benefits, they also bring a number of new and emerging risks. These include risks to privacy and security, misleading and deceptive designs, the potential for diminished choice and product discrimination, as well as uncertainty around accountability, liability and ownership.

Consumer policy makers have recognised the need to keep up with the pace of change inherent to digital transformation. They want to provide well-tailored protections and adequate tools so that consumers can participate effectively in the digital era. Moreover, they increasingly recognise the need to consider behavioural insights and empirical evidence in the design of consumer policies fit for the digital age. To that end, they are drawing on growing evidence that commercial practices exploiting consumer behavioural biases are particularly prevalent on line, especially during the COVID-19 crisis. In this regard, the OECD's consumer behavioural insights work, most recently on personalised pricing and disclosures, can serve as a useful tool for consumer policy makers.

## References

- ACCC (2020), "Advice for older Australians", webpage, <https://www.scamwatch.gov.au/get-help/advice-for-older-australians> (accessed on 21 October 2020). [23]
- ACM (2019), *Protection of the Online Consumer: Boundaries of Online Persuasion*, The Netherlands Authority for Consumers & Markets, The Hague, <https://www.acm.nl/sites/default/files/documents/2020-02/acm-guidelines-on-the-protection-of-the-online-consumer.pdf> (accessed on 21 October 2020). [26]
- Bakos, Y., F. Marotta-Wurgler and D. Trossen (2014), "Does anyone read the fine print? Consumer attention to standard-form contracts", *The Journal of Legal Studies*, Vol. 43/1, pp. 1-35, <http://dx.doi.org/10.1086/674424>. [31]
- Bar-Gill, O. (2012), *Seduction by Contract: Law, Economics and Psychology in Consumer Markets*, Oxford University Press, Oxford. [32]
- Benartzi, S. and J. Lehrer (2017), *The Smarter Screen: Surprising Ways to Influence and Improve Online Behavior*, Penguin, New York. [27]
- Bohn, D. (2019), "The T-Mobile–Sprint merger could mean the end of the physical SIM card", *The Verge*, 26 July, <https://www.theverge.com/2019/7/26/8931784/t-mobile-sprint-merger-esim-justice-department-requirement-sim-card>. [37]
- Calo, R. (2014), "Digital market manipulation", *The George Washington Law Review*, Vol. 82/4, pp. 995-1051, [http://www.gwlr.org/wp-content/uploads/2014/10/Calo\\_82\\_41.pdf](http://www.gwlr.org/wp-content/uploads/2014/10/Calo_82_41.pdf). [49]
- Carroll, G. et al. (2009), "Optimal defaults and active decisions", *Quarterly Journal of Economics*, Vol. 124/4, pp. 1639-1674, <http://dx.doi.org/10.1162/qjec.2009.124.4.1639>. [40]
- CMA (2018), "Pricing algorithms: Economic working paper on the use of algorithms to facilitate collusion and personalised pricing", *Working Paper*, No. 94, Competition & Markets Authority, London, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/746353/Algorithms\\_econ\\_report.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746353/Algorithms_econ_report.pdf). [52]
- Consumers International (2019), *Artificial Intelligence: Consumer Experiences in New Technology*, Consumers International, London, <https://www.consumersinternational.org/media/261949/ai-consumerexperiencesinnewtech.pdf>. [5]
- Consumers International and The Internet Society (2019), *The Trust Opportunity: Exploring Consumers' Attitudes to the Internet of Things*, Consumers International, London and The Internet Society, Reston, Virginia, <https://www.consumersinternational.org/media/261950/thetrustopportunity-jointresearch.pdf>. [8]
- CPSC (2003), *Recall Effectiveness Research: A Review and Summary of the Literature on Consumer Motivation and Behavior*, Consumer Product Safety Commission, Washington, DC, <http://www.cpsc.gov>. [58]
- Dark Patterns (n.d.), *Dark Patterns*, website, <https://www.darkpatterns.org/> (accessed on 21 October 2020). [15]
- European Commission (2019), *Directive of the European Parliament and of the Council amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU as regards the better enforcement and modernisation of Union consumer protection rules*, European Commission, Brussels, <https://data.consilium.europa.eu/doc/document/PE-83-2019-INIT/en/pdf>. [51]
- European Commission (2016), *Study on Consumers' Attitudes Towards Terms and Conditions*, European Commission, Brussels, [http://ec.europa.eu/consumers/consumer\\_evidence/behavioural\\_research/docs/terms\\_and\\_conditions\\_final\\_report\\_en.pdf](http://ec.europa.eu/consumers/consumer_evidence/behavioural_research/docs/terms_and_conditions_final_report_en.pdf). [29]
- European Commission (2011), "Directive 2011/83/EU of the European Parliament and of the Council on Consumer Rights", *Official Journal of the European Union*, No. 22/11, European Commission, Brussels, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0083&rid=1>. [46]
- FTC (2017), *Blurred Lines: An Exploration of Consumers' Advertising Recognition in the Contexts of Search Engines and Native Advertising*, Federal Trade Commission, Washington, DC, [https://www.ftc.gov/system/files/documents/reports/blurred-lines-exploration-consumers-advertising-recognition-contexts-search-engines-native/p164504\\_ftc\\_staff\\_report\\_re\\_digital\\_advertising\\_and\\_appendices.pdf](https://www.ftc.gov/system/files/documents/reports/blurred-lines-exploration-consumers-advertising-recognition-contexts-search-engines-native/p164504_ftc_staff_report_re_digital_advertising_and_appendices.pdf). [35]
- FTC (2016), "Putting disclosures to the test", *Workshop: Staff Summary*, Federal Trade Commission, Washington, DC, <https://www.ftc.gov/system/files/documents/reports/putting-disclosures-test/disclosures-workshop-staff-summary-update.pdf>. [36]
- FTC (2013), *.com Disclosures: How to Make Effective Disclosures in Digital Advertising*, Federal Trade Commission, Washington, DC, <https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf>. [34]
- FTC (2009), *Negative Options: A Report by the Staff of the FTC's Division of Enforcement*, Federal Trade Commission, Washington, DC, <https://www.ftc.gov/sites/default/files/documents/reports/negative-options-federal-trade-commission-workshop-analyzing-negative-option-marketing-report-staff/p064202negativeoptionreport.pdf>. [45]
- Gal, M. and N. Elkin-Koren (2017), "Algorithmic consumers", *Harvard Journal of Law & Technology*, Vol. 30/2, pp. 309-353. [18]

- Johnson, E., S. Bellman and G. Lohse (2002), "Defaults, framing and privacy: Why opting In-opting out", *Marketing Letters*, Vol. 13/1, pp. 5-15, [https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/1173/defaults\\_framing\\_and\\_privacy.pdf](https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/1173/defaults_framing_and_privacy.pdf). [44]
- Johnson, E. and D. Goldstein (2004), "Defaults and donation decisions", *Transplantation*, Vol. 78/12, pp. 1713-1716, <http://dx.doi.org/10.1097/01.TP.0000149788.10382.B2>. [41]
- Johnson, E. et al. (1993), "Framing, probability distortions and insurance decisions", *Journal of Risk and Uncertainty*, Vol. 7, pp. 35-51, [https://www8.gsb.columbia.edu/decisionciences/sites/decisionciences/files/files/Framing\\_Probability\\_Distortions-3.pdf](https://www8.gsb.columbia.edu/decisionciences/sites/decisionciences/files/files/Framing_Probability_Distortions-3.pdf). [43]
- Kahneman, D. et al. (1991), "Anomalies: The endowment effect, loss aversion and status quo bias", *The Journal of Economic Perspectives*, Vol. 5/1, pp. 193-206, [https://scholar.princeton.edu/sites/default/files/kahneman/files/anomalies\\_dk\\_jlk\\_rht\\_1991.pdf](https://scholar.princeton.edu/sites/default/files/kahneman/files/anomalies_dk_jlk_rht_1991.pdf). [38]
- Kovač, M. and A. Vandenberghe (2015), "Regulation of automatic renewal clauses: A behavioural law and economics approach", *Journal of Consumer Policy*, Vol. 38, pp. 287-313, <http://dx.doi.org/10.1007/s10603-015-9286-4>. [48]
- Lester, P. (2019), "Why you can't always trust online customer reviews", *Which?*, 15 March, <https://www.which.co.uk/news/2019/03/why-you-cant-always-trust-online-customer-reviews/>. [17]
- Mathur, A. et al. (2019), "Dark patterns at scale: Findings from a crawl of 11K shopping websites", *Proceedings of the ACM on Human-Computer Interaction*, Vol. CSCW/81, <https://doi.org/10.1145/3359183>. [14]
- OECD (2020), *Protecting Online Consumers During the Covid-19 Crisis*, webpage, <http://www.oecd.org/coronavirus/policy-responses/protecting-online-consumers-during-the-covid-19-crisis-2ce7353c/> (accessed on 21 October 2020). [1]
- OECD (2019), *An Introduction to Online Platforms and Their Role in the Digital Transformation*, OECD Publishing, Paris, <https://doi.org/10.1787/53e5f593-en>. [9]
- OECD (2019), *Challenges to Consumer Policy in the Digital Era: Background Report*, G20 International Conference on Consumer Policy, Tokushima, Japan, 5-6 September, OECD, Paris, <http://www.oecd.org/sti/consumer/challenges-to-consumer-policy-in-the-digital-age.pdf>. [21]
- OECD (2019), *Delivering Better Policies Through Behavioural Insights: New Approaches*, OECD Publishing, Paris, <https://dx.doi.org/10.1787/6c9291e2-en>. [54]
- OECD (2019), *Recommendation of the Council on Artificial Intelligence*, OECD, Paris, <http://dx.doi.org/OECD/LEGAL/0449>. [13]
- OECD (2019), "The road to 5G networks: Experience to date and future developments", *OECD Digital Economy Papers*, No. 284, OECD Publishing, Paris, <https://dx.doi.org/10.1787/2f880843-en>. [4]
- OECD (2019), "Using digital technologies to improve the design and enforcement of public policies", *OECD Digital Economy Papers*, No. 274, OECD Publishing, Paris, <https://dx.doi.org/10.1787/99b9ba70-en>. [11]
- OECD (2018), "Consumer policy and the smart home", *OECD Digital Economy Papers*, No. 268, OECD Publishing, Paris, <https://dx.doi.org/10.1787/e124c34a-en>. [3]
- OECD (2018), "Consumer product safety in the Internet of Things", *OECD Digital Economy Papers*, No. 267, OECD Publishing, Paris, <https://dx.doi.org/10.1787/7c45fa66-en>. [2]
- OECD (2018), "Enhancing product recall effectiveness: OECD background report", *OECD Science, Technology and Industry Policy Papers*, No. 58, OECD Publishing, Paris, <https://doi.org/10.1787/ef71935c-en>. [56]
- OECD (2018), "Improving online disclosures with behavioural insights", *OECD Digital Economy Papers*, No. 269, OECD Publishing, Paris, <https://dx.doi.org/10.1787/39026ff4-en>. [24]
- OECD (2018), "IoT measurement and applications", *OECD Digital Economy Papers*, No. 271, OECD Publishing, Paris, <https://dx.doi.org/10.1787/35209dbf-en>. [19]
- OECD (2018), "Measuring and maximising the impact of product recalls globally: OECD workshop report", *OECD Science, Technology and Industry Policy Papers*, No. 56, OECD Publishing, Paris, <https://dx.doi.org/10.1787/ab757416-en>. [20]
- OECD (2018), *Personalised Pricing in the Digital Era - Note by the United States*, OECD, Paris, [https://www.ftc.gov/system/files/attachments/us-submissions-oecd-2010-present-other-international-competition-fora/personalized\\_pricing\\_note\\_by\\_the\\_united\\_states.pdf](https://www.ftc.gov/system/files/attachments/us-submissions-oecd-2010-present-other-international-competition-fora/personalized_pricing_note_by_the_united_states.pdf). [53]
- OECD (2018), *Personalised Pricing in the Digital Era*, background note by the Secretariat, <http://www.oecd.org/daf/competition/personalised-pricing-in-the-digital-era.htm>. [50]
- OECD (2017), "Trust in peer platform markets: Consumer survey findings", *OECD Digital Economy Papers*, No. 263, OECD Publishing, Paris, <https://dx.doi.org/10.1787/1a893b58-en>. [7]
- OECD (2017), "Use of Behavioural Insights in Consumer Policy", *OECD Science, Technology and Industry Policy Papers*, No. 36, OECD Publishing, Paris, <https://dx.doi.org/10.1787/c2203c35-en>. [25]
- OECD (2016), *Recommendation of the Council on Consumer Protection in E-Commerce*, OECD, Paris, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0422>. [22]

- OECD (2010), *Consumer Policy Toolkit*, OECD Publishing, Paris, <https://dx.doi.org/10.1787/9789264079663-en>. [6]
- Ofcom (2017), *Adults' Media Use and Attitudes*, Ofcom, London, [https://www.ofcom.org.uk/\\_\\_data/assets/pdf\\_file/0020/102755/adults-media-use-attitudes-2017.pdf](https://www.ofcom.org.uk/__data/assets/pdf_file/0020/102755/adults-media-use-attitudes-2017.pdf). [16]
- OFT (2007), "Internet Shopping: An OFT Market Study", webpage, <http://webarchive.nationalarchives.gov.uk/20140402163042/http://oft.gov.uk/OFTwork/markets-work/internet>. [28]
- Packard, V. (1957), *The Hidden Persuaders*, Ig Publishing, New York. [55]
- Richmond, B. (2019), *A Day in the Life of Data*, Consumer Policy Research Centre, Melbourne. [10]
- Samuelson, W. and R. Zeckhauser (1988), "Status quo bias in decision making", *Journal of Risk and Uncertainty*, Vol. 1, pp. 7-59. [42]
- Smith, A. (8 April 2020), "Using artificial intelligence and algorithms", Federal Trade Commission, Business blog, <https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms>. [12]
- Sousa Lourenço, J. et al. (2016), *Behavioural Insights Applied to Policy: European Report 2016*, European Commission, Brussels, <http://dx.doi.org/10.2760/903938>. [47]
- Stark, D. and J. Choplin (2009), "A license to deceive: Enforcing contractual myths despite consumer psychological realities", *NYU Journal of Law & Business*, Spring, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1340166](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1340166). [30]
- Sunstein, C. (2013), "Deciding by default", *University of Pennsylvania Law Review*, Vol. 162/1, pp. 1-57, [http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1000&context=penn\\_law\\_review](http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1000&context=penn_law_review). [39]
- Tversky, A. and D. Kahneman (1981), "The framing of decisions and the psychology of choice", *Science*, Vol. 211/4481, pp. 453-458, <http://links.jstor.org/sici?sici=0036-8075%2819810130%293%3A211%3A4481%3C453%3ATFODAT%3E2.0.CO%3B2-3>. [33]
- Wood, L. (2016), *UK Consumer Product Recall: An Independent Review*, Department of Business Innovation and Skills, Government of the United Kingdom, London, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/509125/ind-16-4-consumer-product-recall-review.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/509125/ind-16-4-consumer-product-recall-review.pdf). [57]





**From:**  
**OECD Digital Economy Outlook 2020**

**Access the complete publication at:**

<https://doi.org/10.1787/bb167041-en>

**Please cite this chapter as:**

OECD (2020), "Consumer policy in the digital transformation", in *OECD Digital Economy Outlook 2020*, OECD Publishing, Paris.

DOI: <https://doi.org/10.1787/7570fa4a-en>

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. Extracts from publications may be subject to additional disclaimers, which are set out in the complete version of the publication, available at the link provided.

The use of this work, whether digital or print, is governed by the Terms and Conditions to be found at <http://www.oecd.org/termsandconditions>.