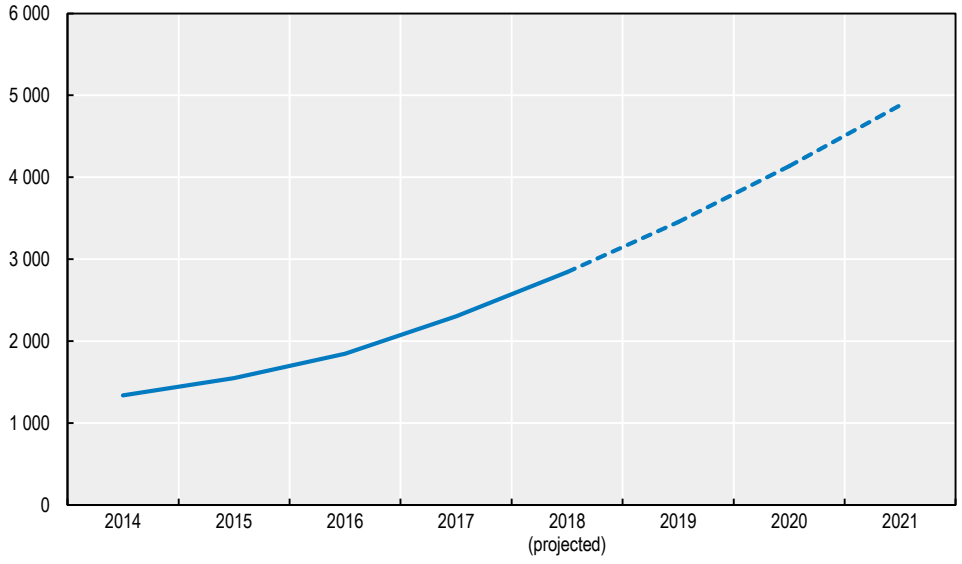
Chapter 5. Trust and online markets

Online markets offer a host of benefits for consumers through innovative and low-cost products. However, online markets can only fulfil their potential if they benefit from consumer trust. Where product information is hard to obtain and assess, markets may not respond to consumer needs. Consumers may be forced to rely on imprecise indicators of quality—such as brand names—to establish trust. This, in turn, limits firms' incentives to improve their offering and deters new entrants. In other cases, consumers may be deterred from using online markets altogether. Establishing an environment of trust in online markets requires multidisciplinary (and often cross-border) approaches from authorities charged with ensuring fair competition, consumer protection, and data protection, as well as other regulators. This chapter considers the benefits and risks associated with online markets from the perspective of trust.

5.1. Introduction

Technological changes are reshaping the functioning of many markets and introducing new ones. Online markets[1] for products offered to final consumers are growing in importance, and have become a key sector of the global economy today (OECD, 2012, p. 5). Activity in these markets, broadly termed e-commerce,[2] has grown significantly, with total worldwide online retail sales increasing from 1.336 trillion US dollars in 2014 to 2.304 trillion US dollars in 2017 (Statista, 2019a). This trend in transaction value is expected to continue, while the number of people around the world buying online is forecast to increase from 1.66 billion in 2016 to over 2.14 billion in 2021 (Statista, 2019b). The digital transformation, and its role in reshaping traditional markets, is here to stay.

Figure 5.1. Total worldwide e-commerce sales (USD billions), 2014-2021



Source: Statista (2019a).

This digital transformation has fundamentally changed how many consumers make purchases and acquire information about products. Consumers can shop from suppliers located anywhere in the world, with only limited constraints due to logistics or regulation. They can also benefit from increased transparency, which enhances choice and may reduce transaction costs considerably (Friederiszick, Glowicka 2016, p. 43).

Online markets do not only allow consumers to shop online for products that they would previously have only found in brick-and-mortar shops, but also to benefit from the creation of new business models and the development of new products. One example is the growth of businesses that offer products at a price of zero in exchange for consumer data or attention to advertising. This latter type of business model existed before the digital economy, and it is typical of the radio, television and newspaper industries. However, the scale at which it occurs in the new digital era and the amount of innovative products that it is generating is different: nowadays, seven out of the ten largest global companies operating in digital markets provide zero-price products (PwC, 2018).

With these benefits also come some challenges. The availability of information, through consumer reviews and rating systems, price comparison websites, or price transparency

between retailers, generally thought to facilitate decision-making, could in some cases be counterproductive. For example, fake or misleading consumer reviews, price comparison websites, and rating systems may hamper consumers' ability to select the product that is right for them (OECD, 2019a). In addition, greater transparency in pricing may be used by suppliers to limit price competition (through resale price maintenance policies imposed on retailers), or to collude among themselves (OECD, 2018a, p. 10).

Further, while consumers can benefit from customised services obtained for a price of zero in exchange for their data, these new business models have raised some privacy and consumer protection concerns to which markets may not be responsive (Stucke and Grunes, 2016, pp. 56-57). In particular, while data is a key unit of exchange in online services, consumers do not appear to consider this in their decision-making, and are in any event given few if any opportunities to make meaningful choices about the terms of this exchange. Limited awareness of how much of their data is collected, how it will be used (e.g. to target advertising or sell to third parties), and the implications of this use, creates significant risks for consumers as well.

Due to these risks and challenges, the role of trust in online markets is particularly important. As with any market, consumers must trust that a product or service provider will fulfil its obligation for the market to function properly. However, with respect to online transactions involving a range of unseen variables, ranging from algorithms that generate personalised pricing, to data collection with privacy implications, trust takes on a new importance in e-commerce. In other words, consumers must have confidence that online markets will develop to bring them a greater range of services in an effective manner and that they will not be exploited when concluding transactions online.

For the purposes of this Chapter, trust in online markets can be defined as the willingness of an online consumer, in the presence of uncertainty, to take the risk of entering into a transaction with an online provider of goods or services.[3] A similar definition is proposed by the OECD: *"From an individuals' point of view, trust in the digital age is about the willingness to risk time, money, and disclosure of personal data to engage in commercial and social activities, and to become vulnerable if a purchase goes wrong or if their data are stolen or if they are used to monitor their behaviour, to discriminate against them or to violate their privacy"* (2019, p. 120).

Uncertainty is a key element of online transactions requiring consumer trust. Consumers may experience uncertainty with respect to the integrity of online transaction systems (such as security breaches in data exchanges or errors in the processing of the transaction) and regarding the behaviour of the players involved (such as the willingness of the supplier to provide a product of quality) (Grabner-Kraeuter, 2002, p. 45). While legal frameworks provide some protection in relation to some aspects of the online transaction, some consumers may be limited in their ability to verify *ex ante* or monitor throughout the transaction the reliability of the supplier. As Head and Hassanein put it: *"Consumers may at first feel a sense of chaos in the e-commerce market, as they fear that their personal information may be stolen due to unreliable security and that online businesses may be fraudulent […] Trust also involves vulnerability. When people trust they expose themselves to risk."* (2001, pp. 11-12).

Given this element of uncertainty and risk, trust is required, first, for consumers to engage in online transactions and to have confidence that online providers are providing complete and accurate information on the characteristics of their products or services, and will fulfil the obligations they undertake.[4] Second, market participants must trust that unlawful behaviour in these markets, such as misleading, fraudulent or abusive conduct, has a high

probability of being detected and punished and that online transactions do not create cybersecurity risks. In addition, society at large expects that online markets are subject to compliance with competition law, data protection, consumer protection and financial regulations. Similarly, both law enforcement authorities and market participants are expected to behave with integrity and enforce or comply with the law. Trust is therefore essential in numerous contexts to support the development of online markets, and their efficient functioning.

While consumers are the most immediately impacted by the trustworthiness of online markets (referred to in other chapters as the trust stakeholder), an insufficient level of trust in a market can have wider implications. For example, SMEs and firms more generally rely on consumer trust to be able to sell their products and services online. Third-parties such as online advertisers and data acquirers also need to be trusted by consumers before establishing of a commercial relationship.

So trust in online markets is crucial in order to create a supportive environment for commerce, but it should not be excessive, i.e. so high that consumers do not critically engage with the information presented to them regarding products or services online. In both cases, the ability of markets to operate competitively and therefore efficiently may be impaired, with significant implications for consumers and economic growth more broadly. Blind trust, defined as "trust in situations that most people would agree do not warrant trust" (Mayer et al., 1995, p. 715) and that may allow exploitation, must be distinguished from informed trust. Vulnerable consumers, who may not have enough information or enough choice, are susceptible to firm misconduct, or at the very least getting a bad deal, if they are blindly trusting in online markets.

No single policy instrument is sufficient to ensure that online markets reach their potential in terms of benefits for consumers. In particular, for consumers to be able to have informed trust in online markets, they must (1) be confident that the boundaries of firm misconduct are clearly-defined and actively enforced, and (2) benefit from enough information and meaningful opportunities to make decisions and get the best deal possible, over and above the minimum legal standards for online products. Competition, consumer protection, data protection and sector regulators all have a role to play, in terms of enforcement, consumer advocacy, and working with policymakers, to promote informed trust.

The structure of this Chapter is as follows:

- Section 2 addresses the reasons why trust plays a prominent role in online markets.
- Section 3 illustrates the potential risks of a loss of trust or of the existence of too much trust in online markets.
- Section 4 identifies the policies that are required to promote an optimal level of informed trust in online markets.

5.2. The role of trust in online markets

As noted above, consumers in online markets face substantial uncertainty, including an inability to inspect physical products before using them, risks of payment methods being compromised, potential privacy violations, and the potential for fraudulent conduct, among others. Thus, trust is crucial for these markets. A 2016 consumer survey conducted by the OECD demonstrated the importance of trust in the minds of digital consumers, especially the role of digital platforms, legal protections, and access to ratings and reviews in promoting that trust (see the "Trust in Peer Platform Markets" report, OECD, 2016b).

Trust may be a particularly important factor for online businesses relying on data collection. A 2012 study found that over 50% of the participants ranked trusting businesses as the most important driver of their willingness to share their data, while over 30% of them agreed that they assigned importance to having previously purchased from a certain brand or business. The study concludes that *"businesses have an obligation to ensure that their brand is trusted by the consumer. If it is not, then the consumer will not feel comfortable in entering into a commercial relationship which requires them to divulge personal data"* (DMA, 2012, p. 16).

The presence of trust is all the more fundamental for the functioning of online markets due to the fact that, in some cases, the interaction between the players involves a considerable divergence of interests between users, suppliers, advertisers and data brokers that operate in them. This principal agent problem may negatively impact consumer trust and either discourage consumers from entering the market or make them too confident on the bona fide of the other players involved.

Misaligned incentives could be found in search engine markets, for instance, where the interest of consumers in terms of accuracy of results may conflict with the supplier's desire to earn revenue by promoting advertiser websites. This in turn may clash with the advertisers' interest to reach users in a more targeted and accurate way (Stucke and Ezrachi, 2016, p. 92).

Therefore, without a desirable degree of trust, online markets are unlikely to work efficiently and maximise consumer welfare. The misalignment of incentives is likely to originate or be exacerbated by other issues, such as information asymmetries, consumers inertia, and consumer behavioural biases that can emerge in online markets. Each of these issues and its implications for consumers' trust are discussed in detail below.

5.2.1. Information asymmetries

Online markets involve considerable information asymmetries between online providers and consumers. For example, some products sold online are considered experience goods or credence goods, i.e. products whose quality can only be evaluated after they are used, or cannot be observed at all (OECD, 2010, pp. 32-33; OECD, 2018b, p. 24). This means that their level of quality may be very difficult to assess for consumers.

When buying physical goods online, one major difficulty that consumers may encounter is the inability to check the merchandise in advance. In addition, differences in consumer protection laws between countries may constitute an important barrier to cross-border sales. There can also be uncertainty about the reliability of the online sellers, especially when it is not an established brand.

Further, consumers face difficulties in understanding the terms of exchange for transactions in which the price is zero, and the consumer instead provides a non-monetary asset, such as access to their data or their attention to advertising. The limits associated with collecting, analysing and applying information about the transaction, the quality of the good or service, and the terms of use in online markets create opportunities for the exploitation of consumers (Acquisti et al., 2015). Pricing algorithms that use data on a consumer's characteristics to develop personalised prices have also become an area of consumer concern (OECD, 2018d).

In order to make informed purchasing decisions when undertaking e-commerce transactions, consumers need relevant and accurate information concerning goods and services and the vendors who are supplying them. Imperfect information may either foster

blind trust or reduce trust on the part of consumers, who may overestimate the value of the online good or service and underestimate that of their privacy or of the data exchanged or vice versa. They may therefore decide whether to engage in an online transaction based on an incomplete cost-benefit analysis. In a 2015 Report by the UK competition authority, it emerged that *"[s]ome consumers identify a 'value exchange' from sharing data, but most feel they lack information on how they benefit and perceive firms benefit more that they do"* (CMA, 2015, p. 106). Another US study conducted in 2015 showed that the vast majority of the respondents (91%) disagreed that: *"[i]f companies give me a discount, it is a fair exchange for them to collect information about me without my knowing"* (Turow et al., 2015, p. 4).

A number of studies also highlight the low level of consumer awareness with regard to data collection. One study shows that, even when available to consumers, the magnitude of information makes it impossible in practice to process it: internet users would need to devote an average of 244 hours per year to consulting terms and conditions of the websites they navigate (McDonald and Cranor, 2008). And even when provided with full information, consumers often find the explanations provided to them unintelligible. Online privacy policy notices may not be sufficient to protect privacy or serve as an effective tool to inform consumers. As noted in a US 2014 Report, *"[n]otice and consent creates a non-level playing field in the implicit privacy negotiation between provider and user. The provider offers a complex, take-it-or-leave-it set of terms, while the user, in practice, can allocate only a few seconds to evaluating the offer. This is a kind of market failure"*.[5]

These studies suggest that many consumers' choices in online markets are not an expression of their preferences and of the minimal value they assign to their own data and their privacy, but may be the result of a lack of understanding of the implications of their online activity (Stucke and Grunes, 2016, pp. 58-61), or a limited ability to influence the terms (Ben-Shahar, 2008). The intangibility of the harm caused by a privacy violation and the opaqueness of the terms of the trade-off are often at the origin of inertia (Acquisti et al., 2015, pp. 509-510) that pushes consumers to either blindly trust the online providers, or avoid purchasing altogether.

Aggravating information asymmetries is the risk that online consumers may experience the problem of "information overload" (OECD, 2018e). Consumers may be unable to process all of the information provided to them, for example as can be the case with terms and conditions regarding the collection of personal data.

When generally unaware or overwhelmed, consumers are unlikely to take actions that reflect their desire for better privacy or data protection. But when provided with clearer information, consumers in some cases seem more prone to engage in a cost-benefit evaluation and to prefer options offering increased privacy protection. One experiment conducted in 2011 asked participants to use an especially created search engine to purchase specific products. At first, the search engine only provided access to the sellers' websites and price information and the main driver of participants' purchasing decisions was price. When the search engine displayed additional clear and easily accessible information about privacy protection, most participants opted to pay a higher price to buy from the sellers affording a higher level of privacy protection (Tsai et al., 2011).

5.2.2. Consumer behavioural biases

In addition to information asymmetry issues, additional demand side problems arise in online markets from some consumer behavioural biases. These biases may "push" consumers to implicitly trust a transaction when caution may be warranted, preventing

fulsome decision-making and creating risks of exploitative conduct. These and other biases are explored in detail in the OECD Digital Working Paper on "Improving Online Disclosures with Behavioural Insights" (OECD, 2018e).

The free effect

One potential phenomenon identified in some studies is the "free effect", where consumers disproportionately value a price of zero at the expense of all other determinants of quality (see, for instance, Shampan'er and Ariely, 2016). Given that many product characteristics, such as consumer data protection, are complex and involve substantial information asymmetries, the impact of the free effect may be particularly acute.

One example is the introduction by Amazon of free shipping in part of Europe. At the time of its adoption, the free shipping offer was not implemented in France due to a programming error. In France, the price of shipping was reduced, but remained positive at 1 French Franc, a minimal amount. While orders skyrocketed in countries where the shipping was free, in France the impact of the shipping cost reduction was negligible (Shampan'er et al., 2007, p. 756).

A zero price could have the powerful effect of leading consumers to implicitly trust an online provider, without giving adequate consideration to the value of the 'exchanged good', such as, for instance, their privacy or data protection. Moreover, firms can use the free effect to their benefit in multi-product offers to block entry of new competitors or to drive out of the market the existing ones, ultimately to the detriment of consumers.

The privacy paradox

While consumers report valuing privacy in a range of surveys, there is mixed evidence regarding whether consumers incorporate these concerns in their behaviour. This phenomenon is known as the "privacy paradox". In particular, consumer purchasing behaviour does not always appear to take account of privacy considerations.

Although consumers seem to have generally become increasingly concerned about how their data is collected and used when accessing online services, they continue to use those services. For example, a US survey revealed that the vast majority of the respondents felt that consumers have lost control over how firms' collect and use personal data, and 80% of those who are active on social networks are concerned about the fact that third parties may have access to the data they share. According to a 2014 survey on internet security and trust, 64% of respondents admitted to being more concerned about privacy in 2014 than they were in the previous year (OECD, 2017a, p. 248). A Eurobarometer report on cybersecurity showed that the main worries of online consumers in the EU are misuse of personal data and the security of online payments (European Commission, 2015). One recurrent issue users mention in relation to e-commerce, as opposed to traditional businesses, is that they *"may not trust Internet transactions more generally"* (OECD, 2017a, p. 208). According to a survey conducted in the United States in 2017, 69% of participants think that there are high risks of hacks and cyberattacks and only 25% of them consider that companies handle personal data in a responsible way. Just 10% of respondents expressed the view that they have full control over their personal data. When asked which types of businesses the participants trusted most, only 13% indicated online retailers and 6% social media.

In spite of these concerns, however, consumers continue to purchase online products and services. The firms providing these services have thrived in recent years and many are

rapidly growing. While in 1995, the largest firms in online markets were Internet service providers, in 2017 the biggest players were online platforms, with Google, Amazon, Facebook, Alibaba, and Uber entering the top 15 (OECD, 2017a, p. 208).

Although evidence is mixed, according to some studies consumers would be willing to pay at least a minimal amount to have access to services guaranteeing more privacy (OECD, 2018b, pp. 26-27). One potential explanation of why consumers' fears may not translate into action is examined in the Section below.

Inertia and the status quo

An important distortion that prevent consumers' preference from being reflected in online market is inertia. Consumers may experience a sense of powerlessness in relation to their privacy and data protection online. In one survey, while most of consumers indicated that they would like to do more to protect their privacy online, only *"24% of adults 'agree' or 'strongly agree' with the statement that: 'It is easy for me to be anonymous when I am online'"* (Madden, 2014). Consumers are also often strongly influenced by default options, showing a lack of propensity to change the status quo (OECD, 2010, pp. 46-47). The commercial importance of the status quo and the lack of consumers' response are demonstrated by the value business place in being the default option, such as, for instance, when search engines compete to be the default choice in a browser (Stucke and Grunes, 2016, p. 121).

5.3. Businesses may therefore have opportunities to exploit consumer inertia

For example, a practice called "shrouding" consists of making the disclosure of terms and conditions for online transactions purposely complex so as to prevent consumers from engaging meaningfully with the information (Gabaix and Laibson, 2005, pp. 2-3 and 25). In addition, to the extent that consumers are able to change their privacy settings, businesses may set the default at a relatively high level of personal data disclosure and sharing, taking advantage of status quo biases (see, for instance, OECD, 2019c, p.29). The Risk of a Loss or an Excess of Trust in Online Markets.

The market characteristics identified above may affect trust in online markets. As a result, they may opt not to participate in these markets or, as seems to be the case in at least some markets, they may choose to purchase online products despite a lack of trust. The latter decision could be the result of 'blind' or 'implicit' trust on the part of consumers, for instance when they prefer to skip reading complicated privacy policies when accessing free services. A lack of trust may therefore either limit the broad economic and consumer welfare benefits of online markets, or it may expose consumers to firm misconduct while limiting competition.

5.3.1. The risk of a loss of trust in online markets

As described in Section 2, the functioning of online markets for consumer goods and services hinges upon trust. Even firms that have not engaged in misconduct could be harmed by a general distrust of online markets. Such an outcome could limit the further adoption of e-commerce, since there is still room to grow: in 2014, three quarters of consumers in the OECD countries went online, but only about 50% of them shopped via the internet (OECD, 2017b, p. 24). More seriously, a sudden loss of trust in response to a prominent incident could cause existing consumers to withdraw from online markets. The consequences may be particularly serious for small- and medium-sized businesses (see, for

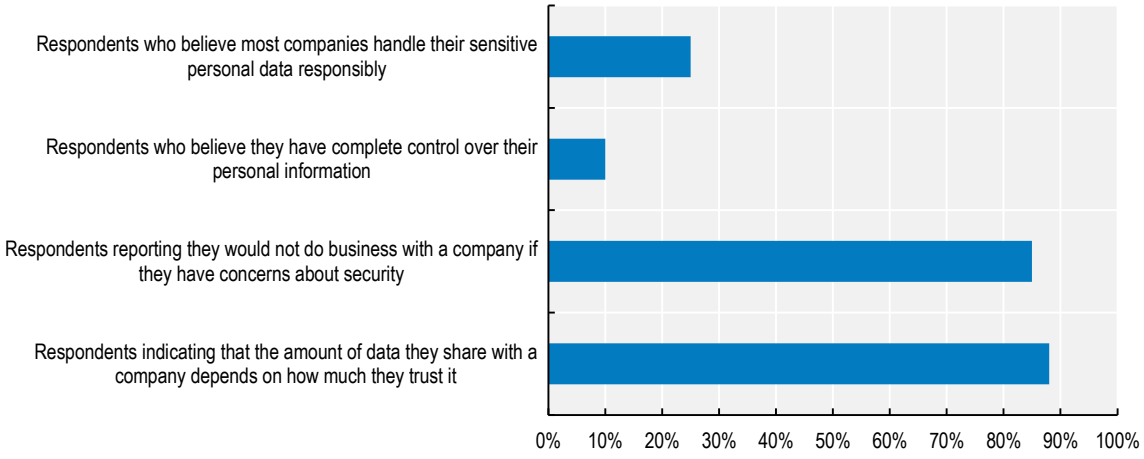
example, OECD, 2019d, p. 158). Thus, without trust, the growth and adoption of new digital markets may be at risk, limiting the ability of these markets to reach their potential in contributing to economic growth and consumer welfare.

Fears of personal data breaches, concerns relating to the complexity of terms and conditions in online purchases or, more generally, the difficulties connected to product liability and consumer guarantees may affect the willingness of consumers to share their data and engage in a transaction (OECD, 2017b, p. 24). For example, around 15% of internet users in the EU28 abstained from purchasing online on account of concerns regarding the delivery or the return of the good in 2017 (OECD, 2019b, p. 126).

Businesses are also exposed to concerns about trust when they make purchases in online markets. Uncertainties about the security of data storage and processing may prevent firms from adopting cloud computing solutions and other digital tools. Data show that SME cloud computing services are underused and that SMEs are not fully informed or fully equipped to manage privacy and security threats (OECD, 2017b, p. 24).

Concerns about trust and the risks of losing it are recognised by at least some digital firms. Consumer surveys corroborate this: in a survey conducted in the United States in 2017, the vast majority of participants indicated they would *"not do business with a company if they had concerns about its security practices"* (see PwC, 2017 and Figure 5.2).

Figure 5.2. Results of a survey of US consumers on trust and data security



Note: Based on a nationally representative sample of 2 000 Americans surveyed through online survey and virtual interviews.
Source: PwC (2017).

5.3.2. The risk of an excess of trust in online markets

An excess of trust may also be problematic in online markets. If consumers are not actively engaged in assessing the online products they use, for example in terms of privacy and data security, advertising content or ease of switching, they are in essence implicitly trusting the firms that supply these products. This is not to say that consumers are at fault, since they may not be supplied with enough accurate information, available information may be difficult to understand, and alternative products may be scarce. While disengagement in these cases is an understandable response, it can contribute to a vicious cycle, as it will

limit the ability of competition to improve the terms offered to consumers while increasing risks of misleading, fraudulent or abusive conduct.

As mentioned above, consumer data plays a fundamental role in many online markets. The complexity of assessing data collection and usage for consumers can, however, be insurmountable. Firms themselves may not know at the time of its collection how a data point will be used, what datasets it will be combined with, who it will be shared with, and whether it can be fully anonymised (or later associated with an individual). Consumers facing this complexity, without the ability to assess the implications of the collection of their data, often choose the blind trust approach of accepting the terms and conditions. They may later fall victim to poor data protection, vague data governance policies, or unexpected consequences such as the use of their data to develop a personalised price.

Another particular risk that may arise in online markets is the manipulation of available information. For example, price comparison websites can have a significant impact on the competitiveness of the market. They have the potential to reduce search, switching and transaction costs for consumers, facilitate market entry and growth, and increase supplier competition. The benefits of digital comparison tools are only felt, however, if they are trustworthy. A recent study by the UK Competition and Markets Authority found that consumers may lack the ability to assess whether these tools are unbiased and may not have a sufficient level of understanding of how they work (CMA, 2017a, p. 70). Some individuals were unaware of the fact that the tools are offered by commercial companies for profit, in some cases as a marketing service for suppliers, and a majority assumed that they are verified and approved by some regulators before going online. In addition, about one third of the respondents admitted that they did not know if digital comparison tools provided full market coverage, i.e. listing of all existing suppliers, when often it is not the case (CMA, 2017b, p. 20).

Another example of the potential inefficiencies brought about by an excess of trust is that of consumer reviews. On the one hand, online reviews may significantly affect consumers' decision-making and, when they are honest, they support trust in online markets, increasing transparency and allowing consumers' to benefit from their peers' perspective on some of the aforementioned uncontrollable aspects of the transaction, such as the risk of non-delivery of goods and of not being able to inspect the goods in advance.

On the other hand, concerns may be raised by the proliferation of misleading reviews. A recent study observed that the speed and rate at which some products sold on Amazon.com are positively reviewed by consumers may be evidence of artificial reviews. According to ReviewMeta, in June, July and August 2017 there was a steep drop in the average review weight, which may suggest that fraudulent reviews were being posted to increase the visibility of certain products. Amazon took steps to ban incentivised reviews and filed lawsuits against more than 1000 individuals and organisations on grounds of review abuse (Woollacott, 2017). Similarly, suspicions arose in relation to the reliability of some TripAdvisor reviews after positive reviews appeared in relation to non-existing restaurants. The Italian competition authority fined the website for improper business practices in 2014, after complaints that the website's content was described as authentic while false reviews had appeared on it.[6] More recently, the Australian competition authority fined Meriton for having manipulated TripAdvisor's reviews of its properties,[7] and an Italian court sentenced to 9 months in prison an individual who sold fake hotel reviews with a false identity.[8] The UK Competition and Market Authority also took action against online fake reviews,[9] and is currently investigating paid for endorsement on social media platforms that influences consumers' buying decisions.[10]

5.4. A policy agenda for trust in digital markets

Trust, and specifically the right amount of informed trust, is crucial for the functioning of online markets. However, as noted above, in some cases consumers have no choice but to blindly trust firms, as they are not given the information or meaningful choices to make an informed decision about the online products they obtain. Other consumers have opted not to use online markets because of a lack of trust. A particularly complex problem may arise, in certain cases, in correctly establishing and attributing the liability for a specific breach of trust in online markets. The rules of allocation of responsibility may vary from country to country (Chun, 2019). Regulation plays a fundamental role in determining who may be responsible for an infringement and in ensuring that adequate mechanisms for redress exist. Policy action can establish and promote informed trust in online markets.

First, consumer and data protection policies can establish minimum acceptable standards, for example with respect to product returns, data governance, and clarity in contractual terms, among others (see OECD, 2018f). These measures require careful design to avoid unintended consequences that stifle innovation and competition – well-crafted approaches can in fact stimulate competition in areas important to consumers, such as privacy. At the same time, enforcement action under existing consumer protection legislation can protect consumers from deceptive, misleading, or fraudulent commercial practices.

Competition authorities can also play an active role in promoting a procompetitive level of trust in online markets. Vigilant enforcement will play a role, but authorities must also use their broader policy toolkit to help inform consumers and provide input on new measures by consumer and data protection authorities. They must also be vocal about making clear that competition is an essential feature of online markets that consumers can trust.

This is borne out by the fact that private initiatives and new business models are already being introduced to bridge some information asymmetries and promote consumer trust. These include, for instance, the development of anonymised features of online digital services, initiatives to enable data portability, voluntary submission to certification schemes, use of third party validated rating and review features, adoption of more favourable data protection or privacy protection terms and conditions, the use of distributed ledger technology or a premium version of a service that guarantees a higher level of privacy protection. It should be noted that this latter option should be intended as offering varied level of privacy above a certain minimum standard of privacy, guaranteed to all consumers.

One recent example is the Tide Foundation, which is using blockchain technology to limit access to consumers' data through encryption, allowing access only to the individual to which the data belong (Shapiro, 2018). This technology would make it possible for businesses intending to target advertisements to a certain category of consumers to use the Tide platform to request data access from users themselves. A choice would then be given to the consumers as to whether to accept to share their data and receive a fair compensation for their use, or to deny approval.

Another example of a private initiative that is not focused on the development of new technologies but on the involvement of consumers to regain trust is the one adopted by TripAdvisor to stop fake reviews. TripAdvisor allows users to mark with a grey flag reviews that seem suspicious or in violation of the website's guidelines.[11] Some websites, such as Fakespot.com and Reviewmeta.com, apply algorithms to analyse reviews and identify unreliable ones.

Further progress in this regard can be encouraged though the competition policy, consumer protection policy, data protection policy, financial consumer protection policy and potential regulatory measures explored below.

5.4.1. Consumer and data protection regulation

A prerequisite for the proper functioning of online markets in a way that engenders consumer trust is the enforcement of consumer protection law. In particular, provisions regarding deceptive advertising, disclosure, product safety, and fraud must be vigilantly applied in online markets. It should be emphasised that a price of zero is generally not a barrier to the legal applicability of these laws (OECD, 2018b).

Box 5.1. The EU General Data Protection Regulation

The General Data Protection Regulation (GDPR), entered into force on 25th May 2018, is aimed at providing individuals a consistent level of data protection throughout the EU. The personal data protected by the Regulation are "*any information relating to an identified or identifiable natural person*", while processing activity is defined as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*" (Article 4).

The GDPR strengthened, in particular, the individuals' right to switching by expressly recognising the right to:

- receive the personal data that have been provided to a natural or legal person "in a structured, commonly used and machine-readable format";
- provide another natural or legal person with those data without hindrance from the former data controller; or
- request that personal data are sent directly from one natural or legal person to the other, if practically possible (Article 20).

In addition to granting the right to portability, this Regulation provides that individuals can ask their data controller to indicate what personal data they hold and ask for their deletion (Article 15 and Article 17). It also redefines the conditions for the provision of consent by individuals, prohibiting default opt-out options, pre-ticked boxes and unclear language (Article 7).

The Regulation provides for the application of significant administrative fines of up to 20 million Euros or, for undertakings, 4% of annual global turnover for the most serious infringements (Article 83).

However, adapting existing consumer protection policies to novel types of digital products will be a challenge. Consumer redress mechanisms may not easily match the cross-border nature of online transactions. Applying consumer protection law to peer-to-peer transaction platforms may not be straightforward (see OECD, 2016b). Enforcing consumer protection rules may also involve some unique challenges. The OECD Recommendation on Ecommerce

(OECD, 2016a), and the OECD Toolkit for Protecting Digital Consumers (OECD, 2018f) provide guidance in addressing these and other challenges. In the financial sector, additional consumer protection strategies have been identified by the G20-OECD Task Force on Consumer Protection, including with respect to financial literacy.[12]

The protection of personal data and privacy are also crucial for the functioning of online markets (OECD, 2018b, pp. 96-97). Rules regarding the disclosure of data collection and use, as well as the data protection responsibilities that are triggered when a firm collects data, are coming into increasing focus. Beyond these fundamental protections, an additional right being implemented by data protection regulators to help increase consumer choices and enable new entry into digital markets is data portability.[13] This measure recognises that limited portability constitutes a significant switching cost for consumers, limiting their ability to get the best deal possible. For example, in the EU, the consumer right to data portability was recently granted by Article 20 of the General Data Protection Regulation.[14]The Australian government has recently proposed the introduction of a new "Consumer Data Right", aimed at facilitating data portability to guarantee to consumers the ability to switch and foster competition.[15] In the context of its market study on digital comparison tools, the UK Competition and Markets Authority (CMA) has recommended exploring the use of data portability to foster competition between these online tools (CMA, 2017a, p. 84).

5.4.2. Financial consumer protection regulation and enforcement

Financial services regulation illustrates the role that sector-specific regulation can play in promoting trust in online markets. Among many other things, critical component is ensuring that oversight bodies, i.e. regulatory or supervisory authorities charged with protecting financial consumers, have adequate supervisory tools and the right mix of resources and capabilities to be able to respond appropriately to new digital business and distribution models.

A key consideration for such oversight bodies is to achieve a balance between the development of technological innovation without undue limitation and ensuring that an appropriate level of financial consumer protection is maintained. Depending on the circumstances, approaches may include establishing mechanisms such as "regulatory sandboxes" to allow new business models to be tested in a controlled environment, "innovation hubs", applying proportionate regulatory requirements and/or providing regulatory support, advice or guidance on the application of the regulatory framework.

Requirements relating to disclosure and transparency are a fundamental part of most financial consumer protection regimes. Technological developments, including the availability of data, provide opportunities to improve disclosure approaches based on a better understanding of consumer decision-making and to explore alternatives. Approaches for consideration by policymakers include, *inter alia*:

- Testing and exploring new ways of making disclosure more effective for consumers in terms of more targeted, proportionate and customer-centric approaches. For example, when designing their online finance platforms or applications, banks in Hong Kong, China should consider the use of tools such as pop-ups and hyper-linked text to provide customers with information to help them to make informed borrowing decisions.
- Encouraging financial services providers to test digital disclosure approaches to ensure their effectiveness, taking into account factors such as different screen sizes, communication formats, different local languages and dialects and the digital

literacy of the target audience for the product. For example, findings from a recent European Commission (2019) study shows that information provided upfront, saliently, early enough in the process, in an engaging format and in a way that aids comparison helps consumers make better choices online, especially those that are vulnerable due to their low digital and financial literacy. The study also confirms that presenting the information in a way that is adapted to the size of mobile screens helps consumers make better choices.

- Technological developments and the increasing availability and use of data also have the potential to create opportunities to explore alternatives to disclosure, for example, via the publication of indicators relating to financial products or services; "smart defaults" where consumers are defaulted to a particular option; or "personalised friction" which allows customers to create steps which act as breaks in a financial transaction.

In relation to the provision of advice, including digital advice, approaches for consideration by policymakers include ensuring that algorithms underlying the generation of digital advice are objective and consistent, and that the methodology underpinning digital advice services is clear and transparent, including options for recourse.

5.4.3. Competition law enforcement

While promoting trust in markets is not an explicit primary goal of competition law, efforts to tackle misconduct or anticompetitive transactions could be broadly beneficial for trust. In particular, enforcement action that protects competition helps ensure that less trustworthy firms are driven out of markets, and new business models that emphasise consumer trust (e.g. data protection-focused offerings) can emerge.

One circumstance in which competition enforcement promotes trust in online markets is when the determinants of trust, such as privacy protections, can be considered elements of quality for the purposes of competition analysis. For instance, and notwithstanding the fact that to date no such case seems to have been brought to the attention of competition authority, the level of privacy or data protection could be limited as a result of a collusive practice by competing companies.

Similarly, the degradation of privacy, data protection or advertisement policies and reduced choice could be the result of an abuse by a dominant firm. Exclusionary strategies may prevent new firms that emphasise privacy protections from emerging. For example, some authors argue that data portability restrictions by firms could qualify as an abuse of a dominant position *"if it can be proved that the dominant company limits markets and technical development to the prejudice of consumers"* (Vanberg and Unver, 2017; Geradin and Kuschewsky, 2016).

Another enforcement example is the German Bundeskartellamt's decision in the *Facebook* case, where the competition authority stated that *"the extent to which Facebook collects, merges and uses data in user accounts constitutes an abuse of a dominant position"*. The decision, focusing on the use of data obtained by Facebook from affiliated companies, such as Instagram, WhatsApp or other websites, rather than on the exclusionary impact on competitors, requires Facebook to i) request user consent for Facebook-owned services to assign collected data to Facebook user accounts; and ii) request user consent for collecting data from other third party websites and assigning them to a Facebook user account.[16]

A worsening of privacy terms and conditions, an increase in advertising content or reduced choices may also be the result of a merger. However, there may be challenges associated

with adopting the right analytical tools for the assessment of mergers effects between online players. One example is the quantification of market shares in zero-price markets, where alternative measures such as the share of users or user interactions may be considered (OECD, 2018b, p. 15). Authorities also face the challenge of assessing mergers that may affect data privacy as one of the possible parameters of competition. For instance, in its decision on *Microsoft/LinkedIn*,[17] the European Commission concluded that the merger could lead to a substantial reduction in consumer choice for professional networks, including with respect to privacy protection. Specifically, the Commission found there were risks that competitors offering better privacy protection could be marginalised following the merger, and therefore required remedies to address these concerns.

5.4.4. Interdisciplinary regulator cooperation and advocacy

The objective of promoting informed trust among consumers in online markets cannot be achieved through a single policy lens, nor will the enforcement of existing rules address all of the concerns and risks outlined above. The OECD E-commerce Recommendation (OECD, 2016b) contains key provisions aimed to build consumer trust in online markets and ensure that consumers benefit from fair business and advertising practices, appropriate disclosures, effective processes for transaction confirmation and payment, measures to address privacy and security risks, product safety, and meaningful access to effective mechanisms to resolve disputes. Other instruments such as the OECD Privacy Guidelines (OECD, 2013) and the OECD Digital Security Risk Management Recommendation (OECD, 2015) underscore the necessity of a coordinated approach to tackle problems arising in online markets, e.g. the security of digital identity in online transactions, digital risk insurance, data governance, data access and portability and algorithmic discrimination (Donohue et al., 2017).

First, there are opportunities for competition, consumer protection, data protection and sector regulatory authorities to coordinate their enforcement efforts by exchanging information, producing joint guidance for the industry, or promoting initiatives aimed at supporting one another in investigations and case management (OECD, 2018b). These opportunities for collaboration can be exploited to promote engaged decision-making by consumers and foster informed trust. For example, competition law remedies aimed at better informing and empowering consumers could be designed with the advice of consumer or data protection authorities. In relation to digital markets, the OECD advocated close cooperation between different authorities in its Recommendation of the Council on Cross-Border Cooperation in the Enforcement of Laws against Spam (OECD, 2006), as did the European Data Protection Supervisor in its 2014 Preliminary Opinion of Privacy and Competitiveness in the Age of Big Data.[18]

Second, regulators can cooperate in terms of their advocacy efforts aimed at better informing consumers and firms. Initiatives to address the asymmetry of information in online markets that have a negative impact on the level of trust could include information campaigns aimed at educating consumers about personal data and privacy. An example for which consumer education is particularly important, and which could benefit from multidisciplinary cooperation, is the financial sector (see Box 5.2).

One advocacy tool that could be particularly effective in identifying issues contributing to trust problems in online markets, and which could serve as a platform for interdisciplinary cooperation, is a market study. Market studies, often carried out by competition authorities, are used when competition law enforcement action is not warranted, but competition does not seem to be functioning properly. They could be used to diagnose problems in markets

and their causes, whether these are related to market failures (including information asymmetries), demand-side problems, unintended consequences of regulation, or firm conduct that is not illegal but which raises policy concerns, among others. Measures to address competition, consumer protection or data protection concerns could be designed, including further advocacy aimed at firms or consumers, or recommendations for policy changes by governments. In a small number of jurisdictions, competition authorities also have powers to impose remedies in the context of a market study. These have been used, for example, to improve the information available to consumers, reduce switching costs, and encourage new entry (OECD, 2018c, p. 4). The German competition authority (Bundeskartellamt) has, for example, recently obtained legislative powers to initiate market studies in cases where substantial consumer protection concerns are identified.[19]

Box 5.2. Consumer financial education measures

In terms of financial education strategies aimed at supporting consumers to become digitally and financially literate, policymakers should develop core competencies frameworks and appropriate financial education material that can contribute to:

- Build trust and promote beneficial use of DFS and related technological innovation.
- Protect consumers and small businesses from vulnerability to digital crime and misuse/mis-selling.
- Empower consumers to counter new types of exclusion due to the potential misuse of data sources, including data analytics and digital profiling.
- Support consumers at risk of over-reliance on easy access to online sources of credit.

Based on these core competencies, the authorities responsible for financial education, in cooperation with relevant stakeholders, should support the effective delivery of financial education through digital and traditional means and address the needs of target audiences through tailored approaches. This should be undertaken in particular by exploiting the advantages of digital delivery.

Digital tools can also improve access to financial education by, for example, making it more affordable and accessible by wider audiences and tailoring financial education to individual needs, through the possibility of setting up profiles or accounts on digital platforms and obtaining personalised information, instruction and advice. (See OECD, 2017c for further resources.)

An example of a market study which dealt with issues of both competition and trust is the UK retail banking market investigation. The UK CMA required banks to implement Open Banking standards (through common digital protocols, called application programme interfaces, or APIs for short) to enable consumers to make more use of their personal financial information and use it, for example, to better manage their money, or to compare products and services on the basis of their individual needs. The success of these remedies hinged largely on consumer trust, as retail banking customers could choose for their data to be shared with selected third parties such as digital comparison tools or money management apps to take advantage of their services without fearing that it would be

compromised.[20] Well-established data governance standards, alongside effective regulation of the selected third parties, was therefore a particular focus.

Third, and finally, interdisciplinary cooperation may be needed to design additional regulatory policy measures when existing enforcement tools and advocacy efforts are not sufficient. For example, the market failures, consumer biases and distortions (e.g. switching costs) described above may prevent market competition from meeting consumer demands.

Regulation and policies can be designed to promote trust through two mechanisms: first, setting the limits of the competitive playing field for firms, allowing consumers to have confidence that, for example, their personal data will be subject to protections and limitations over undue or abusive use via proper data governance; and second, stimulating competition by giving consumers meaningful opportunities to make choices. Potential options may include, for example, the adoption of more protective policies as a default option, or policies that require websites to provide consumers with opt-in instead of opt-out options for data collection (Kerber, 2016, p. 862). Consumer protection policies could benefit from a competition lens to ensure a level playing field, for example between traditional banks and technology firms seeking to provide financial services.

In the longer term, measures to promote more effective online disclosures (see OECD, 2018e), and more comprehensive consumer options that enable an assessment of trade-offs by consumers, are crucial to attain informed trust. For example, in relation to trust issues around personal data, business models could be encouraged that offer a menu of options, such as a premium option that involves a high price in return for limited data collection, a middle of the road option that limits data use, and a discount option that provides free, or even negatively-priced services, in exchange for wide-ranging data use. Designing new regulatory measures will require a careful assessment of likely consumer and firm behavioural responses, and a mix of regulatory perspectives.

Any new regulatory or policy measure should avoid hampering the introduction of trust-enhancing innovations by businesses themselves. As mentioned above, significant innovations are being developed by businesses to foster trust and gain or re-gain consumers' confidence, for instance by applying new technologies to restore control over personal data (see the Tide Foundation example above) or developing solutions to facilitate data portability.[21]

5.5. Conclusions

Online markets offer a host of benefits for consumers by providing with greater choices of new, innovative and often cheaper products. However, these markets cannot fulfil their potential if consumers are unable to trust them. Where product information is hard to obtain and assess, markets may not respond to consumers' needs. Misaligned incentives, information asymmetries and consumer behavioural biases, such as the free effect, the privacy paradox and the inhibiting power of the status quo, can exacerbate these risks.

An atmosphere of informed trust must therefore be a key objective of policymakers. The consequences of a lack of informed trust could stem from two sources: insufficient trust that stifles growth in online markets, with broader economic effects; and blind implicit trust, that makes individual consumers susceptible to misconduct while hampering the ability of competition to deliver the best products and services (evaluated on a range of parameters including, potentially, privacy protection).

To foster informed trust in these markets, it is important that effective competition, consumer protection, and data protection laws are in place and adequately enforced. Enforcement tools alone, however, may not be sufficient to address the online market failures. Cooperation between competition, data and consumer protection authorities, as well as advocacy activity aimed at promoting procompetitive regulatory reform and private initiatives may be crucial in order for consumers to trust that online markets can offer them a fair deal.

Notes

[1] When referring to online markets for the purposes of this Chapter, reference is made to markets where e-commerce products and services are offered to a final consumer. E-commerce in this narrow sense encompasses the purchase and sale online of goods and services such as tangible goods, services for offline consumption (such as hotel bookings and purchase of tickets) and digital content, with the exclusion, for instance, of intermediation services to online retailers or online marketing activities (OECD, 2018, p. 6).

[2] "An e-commerce transaction is the sale or purchase of goods or services, conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders. The goods or services are ordered by those methods, but the payment and the ultimate delivery of the goods or services do not have to be conducted online. An e-commerce transaction can be between enterprises, households, individuals, governments, and other public or private organisations." OECD (2011), p. 72.

[3] This definition of trust in online markets is based on the definition proposed by R. C. Mayer, J. H. Davis and F. D. Schoorman (1995), "An Integrative Model of Organizational Trust", *20 The Academy of Management Review* 3, 709-734, p. 712, as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party".

[4] For instance, at the early stages of the commercial development of the internet, D. L. Hoffman, T. P. Novak and M. Peralta (1999), "Building Consumer Trust in Online Environments: The Case for Information Privacy", *42 Communications of the ACM* 4, 80-85, p. 80, noted that *"the reason online consumers have yet to shop online in large numbers, or even provide information to Web providers in exchange for access to information offered onsite, is because of the fundamental lack of faith that currently exists between most businesses and consumers on the Web today. In essence, consumers simply do not trust most Web providers enough to engage in relationship exchanges with them".* The environment changed, of course, but trust remained a fundamental element in the interaction between internet users and providers.

[5] President's Council of Advisors on Science and Technology (2014), "Report to the President – Big Data and Privacy: A Technological Perspective", https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf, p. 12.

[6] The Guardian (2014), "Italy Fines TripAdvisor €500,000 over False Reviews", https://www.theguardian.com/travel/2014/dec/23/italy-fines-tripadvisor-500000?CMP=aff_1432&awc=5795_1546443330_f62e3f3221f225ded14706ebf1b5dd82; S. Fenton (2015), "TripAdvisor Denies Rating System is Flawed, After Fake Restaurant Tops Rankings in Italy", www.independent.co.uk/life-style/gadgets-and-tech/news/tripadvisor-denies-rating-system-is-flawed-after-fake-restaurant-tops-rankings-in-italy-10354818.html.

[7] The Guardian (2018), "Meriton Fined $3m for Manipulating TripAdvisor Hotel Reviews", www.theguardian.com/travel/2018/jul/31/meriton-fined-3m-for-manipulating-tripadvisor-hotel-reviews.

[8] Reuters (2018), "Man Jailed in Italy for Writing Fake TripAdvisor Review, www.reuters.com/article/us-italy-tripadvisor/man-jailed-in-italy-for-writing-fake-tripadvisor-review-company-idUSKCN1LS2S3.

[9] https://www.gov.uk/cma-cases/potential-fake-online-reviews-search-engine-optimisation-company.

[10] UK Competition and Market Authority case on Social Media Endorsements, www.gov.uk/cma-cases/social-media-endorsements.

[11] The Guardian (2018), "Man Jailed in Italy for Selling Fake TripAdvisor Reviews", www.theguardian.com/world/2018/sep/12/man-jailed-italy-selling-fake-tripadvisor-reviews-promo-salento. TripAdvisor allows users to mark with a grey flag reviews that seem suspicious or in violation of the website's guidelines, for more information, see www.tripadvisorsupport.com/hc/en-us/articles/200614937-How-do-I-report-an-inappropriate-review-.

[12] G20-OECD Task Force on Consumer Protection, www.oecd.org/finance/g20-oecd-task-force-financial-consumer-protection.htm.

[13] See, for instance, L. Zingales and G. Rolnik (2017), "A Way to Own Your Social-Media Data", *New York Times*, www.nytimes.com/2017/06/30/opinion/social-data-google-facebook-europe.html; W. Kerber (2016), "Digital markets, data, and privacy: competition law, consumer law and data protection", 11 *Journal of Intellectual Property Law & Practice* 1, https://doi.org/10.1093/jiplp/jpw150, p. 862- 863; G. Colangelo and M. Maggiolino (2018), "Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook case for the EU and the U.S.", *Stanford-Vienna Transatlantic Technology Law Forum Working Papers*, No. 31, p. 11.

[14] Article 20 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://data.europa.eu/eli/reg/2016/679/oj.

[15] See https://treasury.gov.au/consumer-data-right/ and C. Beaton-Wells (2018), "Platform Power and Privacy Protection: A Case for Policy Innovation", *CPI Antitrust Chronicle*, pp. 6-8.

[16] Press Release www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html and decision of the Bundeskartellamt, 6 February 2019, www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf.

[17] European Commission , 6 December 2016, COMP/M.8124 – Microsoft/LinkedIn, http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf

[18] European Data Protection Supervisor (2014), "Privacy and Competitiveness in the Age of Big Data: the Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy", https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf.

[19] 9th Amendment to the German Competition Act, see for information https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/12_06_2017_Abteilung%20V.html.

[20] UK Competition and Markets Authority Open Banking, www.openbanking.org.uk/about-us/.

[21] See, for example, the Data Transfer Project, https://datatransferproject.dev/.

References

Acquisti, A., L. Brandimarte, G. Loewenstein (2015), "Privacy and Human Behaviour in the Age of Information" *Science,* Vol. 347/6221, pp. 509-514.

Beaton-Wells, C. (2018), "Platform Power and Privacy Protection: A Case for Policy Innovation", *CPI Antitrust Chronicle*.

Ben-Sahar, O. (2008), "The Myth of the 'Opportunity to Read' in Contract Law"*, Law &Economics Working Papers*, http://chicagounbound.uchicago.edu/law_and_economics/549.

Chun, S.-H. (2019), "E-Commerce Liability and Security Breaches in Mobile Payment for e-Business Sustainability", *Sustainability*, vol. 11, p. 13, doi: 3390/su11030715.

CMA (2017a), Digital Comparison Tool Market Study – Final Report, Competition and Markets Authority, https://assets.publishing.service.gov.uk/media/59c93546e5274a77468120d6/digital-comparison-tools-market-study-final-report.pdf.

CMA (2017b), Digital Comparison Tool Market Study – Final Report – Paper A: Consumer Views, Behaviour, and Experiences, Competition and Markets Authority, https://assets.publishing.service.gov.uk/media/59c9356bed915d7bd5d75dda/paper-a-consumer-experiences.pdf.

CMA (2015), "The Commercial Use of Consumer Data - Report on the CMA's call for information", Competition and Markets Authority, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf.

Colangelo, G. and M. Maggiolino (2018), "Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook case for the EU and the U.S.", *Stanford-Vienna Transatlantic Technology Law Forum Working Papers*, No. 31.

DMA (2012), "Data Privacy: What the Consumer Really Thinks", Direct Marketing Association, https://dma.org.uk/uploads/Data%20privacy%20-%20What%20the%20consumer%20really%20thinks%202012_53cfd432518f2.pdf.

Donohue, M., E. Ronchi and L. Bernat (2016), "Bridging policy silos to boost trust online", *OECD Observer,* http://oecdobserver.org/news/fullstory.php/aid/5589/Bridging_policy_silos_to_boost_trust_online.html.

European Commission (2019), "Behavioural study on the digitalisation of the marketing and distance selling of retail financial services", https://ec.europa.eu/info/sites/info/files/live_work_travel_in_the_eu/consumers/digitalisation_of_financial_services_-_main_report.pdf

European Commission (2015), Special Eurobarometer, Cyber Security Report, http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf.

Friederiszick, H. W. and E. Głowicka (2016), "Competition Policy in Modern Retail Markets", *Journal of Antitrust Enforcement,* Vol.4/1, pp. 42-83, https://doi.org/10.1093/jaenfo/jnv030.

Gabaix, X. and D. Laibson (2005), "Shrouded Attributes, Consumer Myopia, and Information Suppression in Competitive Markets", *NBER Working Paper Series*, http://www.nber.org/papers/w11755.

Geradin, D. and M. Kuschewsky, "Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue", https://ssrn.com/abstract=2216088.

Grabner-Kraeuter, S. (2002), "The Role of Consumers' Trust in Online-Shopping", *Journal of Business Ethics*, Vol. 39, pp. 43-50.

Head, M. M. and K. Hassanein (2001), "Trust in e-Commerce: Evaluating the Impact of Third-Party Seals", http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.465.9764&rep=rep1&type=pdf.

Hoffman, D. L., T. P. Novak and M. Peralta (1999), "Building Consumer Trust in Online Environments: The Case for Information Privacy", *Communications of the ACM,* Vol. 42/4, pp. 80-85.

Kerber, W. (2016), "Digital markets, data, and privacy: competition law, consumer law and data protection", 11 *Journal of Intellectual Property Law & Practice* 1, https://doi.org/10.1093/jiplp/jpw150.

Madden, M. (2014), "Public Perceptions of Privacy and Security in the Post-Snowden Era – Summary of Findings", *Pew Research Centre Information and Technology*, www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

Mayer, R.C., J. H. Davis and F. D. Schoorman (1995), "An Integrative Model of Organizational Trust", 20 *The Academy of Management Review* 3, 709-734.

McDonald, A. M. and L. F. Cranor (2008), "The Cost of Reading Privacy Policies" *A Journal of Law and Policy for the Information Society,* Vol. 4/3, https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf.

Murray, A. (2016), *Information Technology Law*, 3rd ed., Oxford University Press.

Nicolau, J. L. and R. Sellers (2012), "The Free Breakfast Effect: An Experimental Approach to the Zero Price Model in Tourism", *Journal of Travel Research*, Vol. 51/3, pp. 243-249.

OECD (2019a), "Roundtable on Online Consumer Reviews: Committee on Consumer Policy Summary of Discussion", https://one.oecd.org/document/DSTI/CP(2019)8/FINAL/en/pdf.

OECD (2019b), "Going Digital, Shaping Policies, Improving Lives", https://doi.org/10.1787/9789264312012-en.

OECD (2019c), "Online Advertising: Trends, Benefits and Risks for Consumers", *OECD Digital Economy Papers No. 272,* https://doi.org/10.1787/1f42c85d-en..

OECD (2019d), *OECD SME and Entrepreneurship Outlook 2019*, OECD Publishing, Paris, https://doi.org/10.1787/34907e9c-en.

OECD (2018a), "Implications of E-Commerce for Competition Policy", DAF/COMP(2018)3, https://one.oecd.org/document/DAF/COMP(2018)3/en/pdf.

OECD (2018b), "Quality Considerations in Digital Zero-Price Markets", DAF/COMP(2018)14, https://one.oecd.org/document/DAF/COMP(2018)14/en/pdf.

OECD (2018c), "Guide on Market Studies for Competition Authorities", DAF/COMP/WD(2018)26, https://one.oecd.org/document/DAF/COMP/WD(2018)26/en/pdf.

OECD (2018d), "Personalised Pricing in the Digital Era", DAF/COMP(2018)13, https://one.oecd.org/document/DAF/COMP(2018)13/en/pdf.

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

OECD (2018f), "Toolkit for Protecting Digital Consumers: A Resource for G20 Policy Makers", www.oecd.org/internet/consumer/toolkit-for-protecting-digital-consumers.pdf.

OECD (2018g), *G20/OECD Policy Guidance on Digitalisation and Financial Literacy,* www.oecd.org/finance/G20-OECD-INFE-Policy-Guidance-Digitalisation-Financial-Literacy-2018.pdf.

OECD (2018h), *G20/OECD Policy Guidance on Financial Consumer Protection Approaches in the Digital Age,* www.oecd.org/finance/G20-OECD-Policy-Guidance-Financial-Consumer-Protection-Digital-Age-2018.pdf.

OECD (2017a), *OECD Digital Economy Outlook 2017*, https://doi.org/10.1787/9789264276284-en.

OECD (2017b), "Going Digital: Making the Transformation Work for Growth and Well-Being", www.oecd.org/mcm/documents/C-MIN-2017-4%20EN.pdf.

OECD (2017c), "G20/OECD INFE report on adult financial literacy in G20 countries", www.oecd.org/daf/fin/financial-education/G20-OECD-INFE-report-adult-financial-literacy-in-G20-countries.pdf.

OECD (2016a), "Consumer Protection in E-commerce: OECD Recommendation", OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264255258-en.

OECD (2016b), "Protecting Consumers in Peer Platform Markets: Exploring the Issues", OECD Digital Economy Papers, No. 253, https://doi.org/10.1787/5jlwvz39m1zw-en.

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris, https://doi.org/10.1787/9789264245471-en.

OECD (2013), The OECD Privacy Framework, including the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

OECD (2012), The Digital Economy, DAF/COMP(2012)22, www.oecd.org/daf/competition/The-Digital-Economy-2012.pdf.

OECD (2011), OECD Guide to Measuring the Information Society 2011, OECD Publishing, Paris, http://dx.doi.org/10.1787/10.1787/9789264113541-en,

OECD (2010), OECD Consumer Policy Toolkit, https://doi.org/10.1787/9789264079663-en.

OECD (2006), "Recommendation of the Council on Cross-Border Cooperation in the Enforcement of Laws against Spam", OECD/LEGAL/0344, https://legalinstruments.oecd.org/public/doc/118/118.en.pdf.

OECD (2002), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Publishing, Paris, https://doi.org/10.1787/9789264196391-en.

PwC (2018), "Global Top 100 companies by market capitalisation: 31 March 2018 update", www.pwc.com/gx/en/audit-services/assets/pdf/global-top-100-companies-2018-report.pdf.

PwC (2017), Consumer Intelligence Series: Protect.me An in-depth look at what consumers want, what worries them, and how companies can earn their trust—and their business, www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html.

Shampan'er K. and D. Ariely (2016), "How Small is Zero-price? The True Value of Free Products", *Federal Reserve Bank of Boston Working Papers*, No. 06-16, www.bostonfed.org/-/media/Documents/Workingpapers/PDF/wp0616.pdf.

Shampan'er K., N. Mazar and D. Ariely (2007), "Zero as a Special Price: The True Value of Free Products", *Marketing Science*, Vol. 26/6, www-2.rotman.utoronto.ca/facbios/file/ZeroPrice.pdf, pp. 742–757.

Shapiro, J. (2018), "Tide Foundation pitches blockchain solution to digital advertising privacy woes", *Financial Review*, www.afr.com/business/media-and-marketing/advertising/the-tide-turns-the-elegant-blockchain-solution-to-20180822-h14cmm.

Statista (2019a), Retail e-commerce sales worldwide from 2014 to 2021, www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

Statista (2019b), Digital buyers worldwide from 2014 to 2021, www.statista.com/statistics/251666/number-of-digital-buyers-worldwide/.

Stucke, M. and A. Ezrachi (2016), "When Competition Fails to Optimize Quality: A Look at Search Engines", *Yale Journal of Law and Technology*, Vol 18/70, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2598128.

Stucke, M. E. and A. P. Grunes (2016), *Big Data and Competition Policy*, Oxford University Press.

Tsai, J. Y., S. Egelman, L. Cranor, A. Acquisti (2011), "The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study", *Information Systems Research*, Vol. 22/2, https://pdfs.semanticscholar.org/e221/d15a4b9f2eb2ab07694aaa584bd59c85532c.pdf, 254-268.

Turow, J., M. Hennessy, and N. Draper (2015), "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation", www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

Vanberg, A. D., M. B. Unver (2017), "The right to data portability in the GDPR and EU competition law: off couple or dynamic duo", *European Journal of Law and Technology*, Vol. 8/1.

Woollacott, E. (2017), "Amazon's Fake Review Problem is No Worse than Ever, Study Suggests", www.forbes.com/sites/emmawoollacott/2017/09/09/exclusive-amazons-fake-review-problem-is-now-worse-than-ever/#32b58b247c0f.

Zingales, L. and G. Rolnik (2017), "A Way to Own Your Social-Media Data", *New York Times*, www.nytimes.com/2017/06/30/opinion/social-data-google-facebook-europe.html.