OECD publishing

GOOD PRACTICE GUIDE ON CONSUMER DATA

OECD DIGITAL ECONOMY PAPERS
September 2019 **No. 290**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This paper aims to complement the OECD *Recommendation of the Council on Consumer Protection in E-Commerce* (E-Commerce Recommendation) and discuss consumer policy issues associated with consumer data practices, offering greater insights into how consumer protection authorities can and have applied the principles in the E-commerce Recommendation to address those issues. The guide focuses on selected consumer data practices, including: i) deceptive representations about consumer data practices; ii) misrepresentations by omission; and iii) unfair consumer data practices. It then provides key business tips to comply with consumer protection principles under the E-commerce Recommendation.

This paper was prepared by Akira Yoshida under the supervision of Michael Donohue and Brigitte Acoca, of the OECD Secretariat. The author acknowledges efforts made by a number of jurisdictions to provide input to the guide, which helped provide the paper with a richer diversity of good practices. It was approved and declassified by the Committee on Consumer Policy by written procedure on 14 August 2019 and prepared for publication by the OECD Secretariat.

This publication is a contribution to the OECD Going Digital project, which aims to provide policymakers with the tools they need to help their economies and societies prosper in an increasingly digital and data-driven world.

For more information, visit www.oecd.org/going-digital. #GoingDigital

Note to Delegations:

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

DSTI/CP(2018)17/FINAL

Table of Contents

Box

1. Introduction

Consumer data flows throughout the economy, powering much of the digital transformation that has taken place over the last decade as well as emerging developments in Artificial Intelligence (AI), predictive analytics and automation that will increasingly affect consumers' lives. Consumers have already benefited from new and enhanced goods and services that have been developed using consumer data. For instance, the proliferation of Internet of Things (IoT) products and voice-controlled digital assistants using AI technologies and providing automatic decision-making systems, have already yielded positive benefits for consumers (OECD, 2018[1]; OECD, 2019[2]; OECD, 2019[3]).

Personalised online content and recommendations have brought better user experience to consumers, in return for sharing their consumer data, including their location information and allowing the tracking of their online activities. In addition, so-called "free" services that are provided in exchange for consumer data are widely appreciated by consumers (Consumer Policy Research Centre, 2019[4]). These developments are likely to further accelerate the use of consumer data in the future (OECD, 2018[5]).

Despite these consumer benefits, the extensive gathering of consumer data raises privacy and security risks. In response, many countries have updated or enacted privacy and data protection laws. These laws are generally based on fair information principles such as those set out in the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, 2013[6]). The Guidelines contain requirements for businesses' data practices, and provide for enforcement structures, remedies such as fines and penalties, and data transfer mechanisms.

In addition to complying with privacy and data protection laws, which are not the focus of this paper, businesses collecting and using consumer data must also take into account consumer protection laws, which prohibit deceptive, misleading, and unfair business conduct. Indeed, in the digital sphere, many business practices may raise not only issues covered by privacy and data protection laws but also by consumer protection laws. The International Conference of Data Protection and Privacy Commissioners (ICDPPC), an organisation of privacy and data protection authorities from across the globe, has actually recognised that "(h)armful, deceptive, or misleading privacy practices can result in situations that raise concerns and lead to enforcement action under both privacy and consumer protection legislation" (ICDPPC, 2018[7]).

To address these consumer concerns, new provisions on the collection and use of consumer data in online transactions have been added to the OECD's *Recommendation of the Council on Consumer Protection in E-commerce* (OECD, 2016[8]) ("E-commerce Recommendation"). For example, the E-commerce Recommendation provides that businesses should not engage in deceptive practices related to the collection and use of consumers' personal data (para. 8) (see Annex A). The provisions under the E-commerce Recommendation apply to e-commerce transactions regardless of whether a monetary payment is involved (see Annex B).

For the purposes of this guide, consumers' personal data ("consumer data") means any information related to an identified or identifiable consumer (an adaptation of the definition of "personal data" in the OECD's Privacy Guidelines) (OECD, 2013[6]). This may include, for instance, the following types of data (OECD, 2013[9]):

- User generated content, including blogs and commentary, photos or videos.
- Activity or behavioural data, including what people search for and look at on the Internet, what people buy online, as well as how much and how they pay.
- Social data, including contacts and friends on social networking sites.
- Locational data, including residential addresses, GPS and geo-location (e.g. from cellular mobile phones), or IP address.
- Demographic data, including age, gender, race, income, sexual preference, and political affiliation.
- Identifying data of an official nature, including name, financial information and account numbers, health information, national health or social security numbers, and police records.

Businesses collect and use consumer data in different ways. They can collect data directly from consumers through a sign up or registration process for a good or service. In addition, they may collect data indirectly from information generated by consumers as they use the good or service. Data can also be inferred from the aggregation of data that consumers actively and passively provide to businesses and other data sources.

Businesses use consumer data for a variety of purposes. These include business-related purposes, such as order fulfilment, improved product performance and development, customer experience improvements, authentication, digital security and fraud detection, and compliance with legal requirements. They may also use it for the dissemination of targeted advertising. Businesses may also collect and use data for other purposes that are not relevant to the services they provide to consumers, such as for sale to third parties.

With this in mind, this guide discusses the consumer policy issues associated with consumer data practices and aims to offer greater insights into how consumer protection authorities can and have applied the principles in the E-commerce Recommendation to address those issues. The guide does not offer specific guidance from privacy and data security perspectives, which are the subject of other OECD Recommendations.

The guide focuses on selected consumer data practices, including: i) deceptive representations about consumer data practices; ii) misrepresentations by omission; and iii) unfair consumer data practices. At the beginning of each chapter, key business tips have been included, some of which may be legally required in some jurisdictions (see Box 1).

Box 1. Summary of key business tips

Deceptive representations about consumer data practices

- Be transparent about your data practices.
- Honour the promises you make to consumers about how you collect, use, and secure their data, and respect their privacy choices.
- Make sure any claims about privacy and data security practices and commitments are accurate and truthful.

Misrepresentations by omission

- Tell consumers the full story about how their data will be collected and handled.
- Make it easy for consumers to find and use the privacy mechanisms you offer.
- Do not bury important information in links to privacy policies or terms and conditions.
- Do not use hard-to-understand legal terms or jargon to obscure your practices.

Unfair consumer data practices

- Treat consumers and their data in accord with fair business practices and consistent with their privacy choices.
- Do not share consumer data with third parties or others that may use it for fraudulent or deceptive purposes.
- Take care when sharing data to prevent others from using that data to target and prey on vulnerable consumers.

2. Deceptive representations about consumer data practices

2.1. Business tips

- Be transparent about your data practices.
    - Use clear language to explain what consumer data you collect, and how you use, share, store and secure it.
    - Make sure you call attention to important information.
- Honour the promises you make to consumers about how you collect, use, and secure their data, and respect their privacy choices.
- Make sure any claims about privacy and data security practices and commitments are accurate and truthful.

2.2. Overview of the issue

Providing consumers with adequate disclosures about consumer data collection and use has become an important consideration that can inform and influence consumers' purchasing decisions. Businesses may therefore advertise to consumers how they process or secure consumer data for their products or services (ICDPPC, 2018[7]).

Deception may occur when consumers are misled by businesses' false or misleading claims into providing consumer data that they would not otherwise have provided. In some jurisdictions, such as Canada, a business representation that is false or misleading and material to the consumer's decision, is illegal, irrespective of whether any consumer has actually been misled.

Businesses may, for example, deceive consumers through false or misleading claims about the type of data collected, the purpose of data gathering, and the way the data is used, shared, retained and erased. Businesses may promise that they will only use consumer data for a certain purpose or time period, or limit data sharing with third parties, or protect it using state of the art security measures, but fail to do so. All of these practices breach material promises to consumers, and therefore could be deemed deceptive (US FTC, 2016[10]; Competition Bureau Canada, 2017[11]; Competition Bureau Canada, 2018[12]).

A privacy choice mechanism that does not in fact offer a meaningful option to consumers could also be regarded as a deceptive practice (US FTC, 2016[10]). Likewise, a practice whereby a business that represents that it complies with privacy-protective certifications, data transfer schemes, or other industry codes on data privacy and security but does not actually do so, may be regarded as misleading or deceptive (UK CMA, 2015[13]; US FTC, 2016[10]).

2.3. Examples

A study by the Norwegian Consumer Council found that the dating app Happn did not act in accordance with its terms of use on data processing. Happn promised (in the Apple App Store and on Google Play) not to share data or user identity with third parties. However, the study found that Happn actually shared key user data with the tracking firm UpSight.

Such shared data included name, age, workplace and gender that were derived from the users' Facebook accounts (Norwegian Consumer Council, 2016[14]).

In 2017, the Federal Trade Commission of the United States (US FTC) charged that the ride-sharing company Uber deceived consumers about its privacy and data security practices. The US FTC's complaint alleged that Uber failed to live up to its claims that the company monitors employee access to consumer data and to reasonably secure sensitive consumer data stored in the cloud. It alleged that Uber had suspended its use of an automated monitoring system after less than a year, and had rarely monitored internal access to data about users and drivers. Under the initial settlement agreement, Uber agreed not to misrepresent how it monitors internal access to consumer data and how it protects and secures that data. The FTC also required Uber to implement a comprehensive privacy program and to provide the agency with regular and independent audits (US FTC, 2017[15]).

In 2018, following Uber's failure to report a significant breach of consumer data to the authority during the previous investigation, the US FTC announced a revised settlement with the company providing that Uber could be subject to civil penalties if it failed to notify the agency of a data breach, and prohibiting the company from misrepresenting how it monitors internal access to consumer data and the extent to which it protects the privacy, confidentiality, security, and integrity of such information. In addition, it required Uber to implement a comprehensive privacy program and to be provided for 20 years with biennial independent and third-party assessments certifying that the company has put in place a privacy program that meets or exceeds the requirements of the US FTC's order (US FTC, 2018[16]).

Failure to follow a consumer's choice may also be a deceptive practice. In 2019, Facebook agreed to pay the US FTC a record-breaking USD 5 billion and fundamentally restructure its privacy practices to settle charges that the company repeatedly used deceptive disclosures and settings, as well as making misleading statements, to undermine users' privacy preferences in violation of a previous FTC order and the FTC Act. Among other deceptive statements, the company claimed that users could restrict the sharing of their information to their Facebook "friends", when, in fact third-party developers could access and collect users' data through their friends' use of third-party developers' apps (US FTC, 2019[17]).

In another case, the US FTC took action against a marketing company that allegedly used tracking technologies through their mobile applications even after consumers opted out of such tracking by blocking or limiting cookies as provided by the company's privacy policy. The US FTC ordered the company to provide an effective opt-out for consumers and offer a prominent hyperlink on its home page explaining what information the company collects and uses for targeted advertising (US FTC, 2017[18]).

Misrepresentations about participation in industry-led or international privacy codes may also be deceptive. For example, the US FTC took action against ReadyTech Corporation over allegations that it falsely claimed it was in the process of being certified as complying with the EU-US Privacy Shield framework, which establishes a process to allow companies to transfer consumer data from EU Member States to the United States in compliance with EU law. While the company initiated an application to the US Department of Commerce in October 2016, it did not complete the steps necessary to participate in the Privacy Shield framework (US FTC, 2018[19]). Since the Privacy Shield Framework went into effect in 2016, the US FTC has brought enforcement actions against ten companies for similar deceptive conduct, including a recent administrative order against data analytics company, Cambridge Analytica (US FTC, 2019[20]).

3. Misrepresentations by omission

3.1. Business tips

- Tell consumers the full story about how their data will be collected and handled.
    - Inform consumers of privacy and data security practices, before asking them to make a material decision.
    - If your business derives revenue from the use of consumer data, do not conceal that from consumers when offering free services.
- Make it easy for consumers to find and use the privacy mechanisms you offer.
    - Design simple and easy-to-use privacy mechanisms.
- Do not bury important information in links to privacy policies or terms and conditions.
- Do not use hard-to-understand legal terms or jargon to obscure your practices.

3.2. Overview of the issue

Businesses may deceive consumers by omitting information about data processing practices that is material to a consumer's decision on whether to enter into a transaction, including for the purpose of acquiring "free" products. For example, failure to disclose information, such as functionalities involving geo-location tracking for marketing purposes and tracking of online activities, may constitute deception.

Likewise, using consumer data in a way that a consumer is not informed about may be misleading, even if the privacy policy is factually correct (UK CMA, 2015[13]). Disclosing material information concerning data collection and use practices only in the terms and conditions may also be misleading, particularly if these terms go beyond what a consumer would reasonably expect (Competition Bureau Canada, 2017[11]). In some jurisdictions, consumers may furthermore be found to be misled when they are asked to consent to changes in the use of the products they have acquired unless they provide their data, fearing that they might otherwise lose access to the products (Italian Competition Authority, 2017[21]).

A closely related and still emerging issue is a misleading "free" claim in non-monetary transactions. The fact that consumer data has been collected with the intention to be used by the business for commercial purposes may be material to the transactional decision from the consumers' perspective, even in non-monetary transactions (see Annex B). Therefore, hiding such an intention to consumers and advertising a service merely as "free" may be considered deceptive in some jurisdictions (UK CMA, 2015[13]). Arguably, some academic observers have asserted that, in some jurisdictions, advertising goods and services as "free" whilst consumers in return are to provide their data or are exposed to ads, could be considered deceptive (Helberger, Borgesius and Reyna, 2017[22]).

It should however be noted that in a number of jurisdictions, the question of whether promoting non-monetary transactions as "free" is misleading, is still being discussed. Given that consumers may have different views and expectations about data practices in

goods or services provided without monetary consideration, there is an ongoing debate as to whether the omission of information on consumer data practices in non-monetary transactions could actually amount to material information under the deception theory. In addition, whether the "free" claim is a misrepresentation by omission may depend on the context and hence require a fact-dependent analysis.

3.3. Examples

In the United States, the FTC reached an agreement with VIZIO, a manufacturer and marketer of internet-connected televisions, which allegedly collected viewing data without informing consumers and seeking their consent. According to the US FTC's complaint, VIZIO's smart TVs automatically tracked what consumers were watching and transmitted such data back to its servers. In addition, VIZIO allegedly also collected and added specific demographic information to the viewing data, such as sex, age, income, marital status, household size, education level, home ownership, and household value. According to the complaint, VIZIO sold this information to third parties, who used it for various purposes, including targeting advertising to consumers across devices. The US FTC entered into a consent agreement with the company, requiring VIZIO to prohibit misrepresentations about the privacy, security, or confidentiality of the consumer data they collect (US FTC, 2017[23]).

In 2016, the Norwegian Consumer Council found that a fitness app, Runkeeper, collected consumer data about its users when the app or handset was not in use, and sent the data to third parties. This practice was not explained in its terms of service, and its users had not given their consent to providing their data in such circumstances. Following the release of the report, Runkeeper announced that they had fixed the bug that *"inadvertently caused the app to send location data to the third-party service"* (Norwegian Consumer Council, 2016[24]; Norwegian Consumer Council, 2016[25]).

In 2019, the Australian Competition and Consumer Commission (ACCC) instituted proceedings before the Federal Court against HealthEngine Pty Ltd (HealthEngine), an online health booking platform, alleging that the company had engaged from 30 April 2014 to 30 June 2018 in a misleading and deceptive conduct by sharing information, such as names, phone numbers, email addresses, and date of birth, of over 135 000 patients with private health insurance brokers for a fee, without adequately informing consumers about it (ACCC, 2019[26]).

In Canada, as part of an investigation in relation to a data breach by Avid Life Media Inc. (ALM), the privacy authority examined the information provided by the company's to its users concerning its consumer data processing practices. The investigation found that the company did not provide key information that could influence a consumer's decision on whether to enter into a transaction. For instance, the company did not disclose the fact that consumers had to pay for the deletion of their consumer data from the service. Based on these findings, the investigation suggested that the omission of material information, as well as other misrepresentations, may question the validity of the consumer consent to the company's consumer data practices (Office of the Privacy Commissioner of Canada, 2016[27]). The US FTC similarly took action against ALM alleging that while the company had claimed that they would delete all of the information of consumers who utilised their Full Delete service, they had failed to do so, retaining the consumer's information for up to a year (US FTC, 2016[28]).

The Hungarian Competition Authority (GVH) reached an agreement in 2018 with Google regarding the processing of consumer data on "Allo", an instant messaging mobile app. The GVH found that Google had not provided sufficient information about the processing of consumer data in the advertisement, installation and application of Allo chatclients. The commitments undertaken by Google required it to set up a page providing information on its data processing practices under the "Allo Help" website, accessible both from the installation process of Allo and from the description available in GooglePlay and the iOSAppStore. Google agreed to develop this page in plain language. Furthermore, the company committed to provide this information in an easily accessible manner (GVH, 2018[29]).

In the United Kingdom, the Competition and Markets Authority (UK CMA) reached an agreement in 2018 with an online dating service provider, Venntro, to require it to provide its customers with clearer information on how their information is shared with other dating websites and whether they have control over how widely their profiles are shared within a network. It also agreed to provide clearer information on its consumer data practices, including processes for cross-registration between the websites and the deletion of dating profiles (UK CMA, 2018[30]).

In 2017, the Italian Competition Authority (AGCM) closed formal proceedings against WhatsApp, following the acquisition of the messaging platform by Facebook. The investigation examined the sharing of consumer data between WhatsApp and Facebook. The AGCM noted that WhatsApp had de facto forced WhatsApp Messenger's users to accept the new Terms of Service, including the provision to share their consumer data with Facebook, by hiding important information about its customers' ability to continue using the service and hence misleading them into believing that, without granting their consent, they would not be able to use the service. According to the AGCM, such practice was implemented through:

- an emphasis on the need to subscribe to the new conditions within the following 30 days, after which time the service would become unavailable
- a lack of information about the potential consequence of denying consent to share consumer data with Facebook
- setting the opt-in option to share the data as the default.

The AGCM found that these practices were unfair and imposed a fine on the company (AGCM, 2017[31]). In another case, the AGCM found that Facebook engaged in an aggressive practice and exerted undue influence on registered consumers by transmitting their data without their express and prior consent to third-party websites/apps for commercial purposes, and vice versa. The undue influence was caused by the pre-selection by Facebook of the broadest consent to data sharing. When users would try to limit their consent, they would face significant restrictions on the use of the social network and third-party websites/apps, inducing them into maintaining the default choice (AGCM, 2018[32]).

In 2017, the EU Consumer Protection Cooperation network took action against Facebook to ensure more transparency with its terms and conditions, including information about its business model and its use of user data for the purposes of service performance and other commercial services. In response, Facebook agreed to modify its terms and conditions, clarifying that user data and content are used *"to improve their overall experience"*, and that its commercial use of user data constitutes an important source of its revenues (EC, 2017[33]). In 2019, the European Commission (EC) and EU consumer authorities reached agreement with Facebook to revise its terms of use to explain how the company uses

consumer data to develop profiling activities and target advertising to finance the company. The new terms will have detailed information on what services Facebook sells to third parties, how consumers can close their accounts, and under what reasons accounts can be disabled (EC, 2019[34]).

In 2018, the International Consumer Protection and Enforcement Network (ICPEN) led an international sweep, identifying a lack of information on apps' collection and processing of consumer data. The ICPEN later published an open letter to businesses on terms and conditions in the digital economy which highlights the importance of clearly explaining what information is collected about consumers and what is done with that information (ICPEN, 2018[35]).

In 2019, as a follow-up to the ICPEN's work, consumer authorities from 27 jurisdictions sent an open letter to Apple and Google to suggest changes to the layouts of their app stores to improve information provided on the use of consumer data. In the letter, the authorities noted the absence of important information on the use of data by the app on the app's main product page in the Google Play Store and Apple App Store. In addition, the authorities have called on businesses to provide the information on consumer data handling upfront in a clear and comprehensive manner. These concerns have not yet been resolved (Authority for Consumers and Markets (Netherlands), 2019[36]; Norway Consumer Authority, 2019[37]).

In Mexico, under the country's Federal Consumer Protection Law, the Federal Consumer Protection Agency (PROFECO) has undertaken monitoring of e-commerce websites, looking in particular into whether their privacy notices explain how they will handle consumer data (PROFECO, 2019[38]).

In some jurisdictions, the omission of material information on business motives in collecting consumer data in non-monetary transactions has been subject to enforcement actions taken by consumer authorities and consumer organisations. For instance, in 2016, a German court granted an injunction against Facebook sought by the Federation of German Consumer Organisations (vzbv), on the basis of EU's unfair commercial practices directive, for its claim that its service is "for free" or "without charge". This was seen by vzbv as a misleading claim as Facebook derives almost all of its revenues from monetizing consumer data for advertising. The case is still ongoing (EC, 2016[39]; vzbv, 2018[40]).

Likewise, in 2018, the Italian Competition Authority fined Facebook for emphasizing the free nature of the service but not the *"commercial objectives that underlie the provision of the social network service, thus inducing users into making a transactional decision that they would not have taken otherwise (i.e. to register in the social network and to continue using it)"* (AGCM, 2018[32]).

4. Unfair consumer data practices

4.1. Business tips

- Treat consumers and their data in accord with fair business practices and consistent with their privacy choices.
- Do not share consumer data with third parties or others that may use it for fraudulent or deceptive purposes.
- Take care when sharing data to prevent others from using that data to target and prey on vulnerable consumers.

4.2. Overview of the issue

In some cases, consumer data practices may run afoul of the fair business principles under the E-commerce Recommendation, or breach fairness requirements in consumer protection laws. Indeed, some jurisdictions prohibit or are seeking to prohibit certain data collection and use practices under unfair business practice theories. It should however be noted that the degree to which a business practice may be deemed unfair may vary significantly from one jurisdiction to another.

In the United States, for example, unfairness occurs when a business practice causes substantial consumer harm, consumers cannot avoid the injury, and the injury is not outweighed by benefits to consumers or competition. The more sensitive the information businesses collect and use (such as social security numbers and medical information), the higher the expectation to treat these consumer data with reasonable security measures (US FTC, 2016[10]). In the European Union, "misleading practices" are a subcategory of "unfair practices" under the Directive on Unfair Commercial Practices (European Parliament, n.d.[41]).

In addition, a business collecting and sharing consumer data with third parties knowing that the third parties intend to use the data in a fraudulent and harmful way may regarded as engaging in unfair practices. This would for example be the case if consumer data obtained by third parties was used to prevent consumers from recognising fake reviews (Competition Bureau Canada, 2017[11]). Arguably, a provision enabling a business entity to change its terms of use or privacy policy unilaterally without a valid reason may also amount to an unfair business practice under unfair contract terms laws (UK CMA, 2015[13]).

There is also the concern that some businesses might use consumer data to prey on vulnerable consumers. For instance, online browsing history could be used in a targeted campaign to identify a potential victim, and this information could be used to mislead the consumer into providing sensitive information such as a bank account or other confidential information (Competition Bureau Canada, 2017[11]). Arguably, the increasing ability of businesses to target online advertising using richer consumer data and profiling could enable businesses to take advantage of other types of consumer vulnerabilities. This kind of practice, however, has not been observed at scale (OECD, 2019[42]).

More generally, data gathering practices by businesses, especially online platforms, may lead to information asymmetries and bargaining power imbalances in the relationship

between consumers and businesses that may violate consumer protection and other laws (ACCC, 2019[43]).

4.3. Examples

Typically, consumers are not in a position to determine if a business is selling their data for fraudulent purposes or sharing their sensitive data. Therefore, consumers should reasonably expect that businesses take the necessary steps to protect their data. To meet such expectations, in some jurisdictions, unfairness protections have been used to address unfair privacy and data security practices. The US FTC (2015[44]) brought a number of enforcement actions against such practices, including:

- financial harm faced by consumers as a result of unreasonable data security
- the sharing of financial account data with scammers
- the use of software to illegitimately gather consumers' sensitive data, location, and even photos in their homes.

In addition, in 2014, the US FTC took action against a data broker, LeapLab, which had sold sensitive consumer data of hundreds of thousands of consumers to scammers who allegedly debited millions from their accounts. The agency found that the data broker had collected payday loan applications of financially strapped consumers, and had then sold that information to marketers whom the company knew had no legitimate need for it. These applications contained the consumer's name, address, phone number, employer, Social Security number, and bank account number. The settlement prohibited the defendants from selling or transferring sensitive consumer data about consumers to third parties and required them to delete any consumer data in their possession (US FTC, 2014[45]; US FTC, 2016[46]).

In 2018, the EC, together with EU consumer authorities, reached an agreement with Facebook, Twitter and Google+, to make their terms of service and payment terms aligned with EU consumer protection rules. Agreed commitments from the companies include providing consumers with a reasonable notice about any change in the existing terms. Facebook agreed to notify its users 30 days in advance of any change in its terms of service or payment terms (EC, 2018[47]).

In 2019, consistent with the agreement reached by the EC, Facebook amended its terms of use to limit its power to unilaterally change its terms and conditions. According to the agreed commitments, changes to its terms and conditions will be allowed if they appear to be reasonable, and the company takes into account the interest of the consumer (EC, 2019[34]).

As a potential response to the significant information asymmetries and bargaining power imbalances between consumers and digital platforms for their collection, use and disclosure of consumer data, the ACCC is considering adopting an unfairness provision under the Australian Consumer Law. According to the proposal, this provision will make unfair contract terms (which are already covered in the Australian Consumer Law), including the terms of use of privacy policies, illegal and subject to civil pecuniary penalties (ACCC, 2019[43]).

In Mexico, the Federal Consumer Protection Law includes provisions regarding the protection of consumer data; guidance principles on the implementation of the provisions in the law are being developed, calling on businesses engaging in e-commerce to implement appropriate and reliable security measures to protect consumer data (PROFECO, 2019[38]).

Annex A. Selected key provisions of the E-commerce Recommendation

Fair business and marketing principles under the E-commerce Recommendation cover the entire business-to-consumer online transactions, including consumer data processing by businesses. Specifically, the principles provide that:

- *Businesses should pay due regard to the interests of consumers and act in accordance with fair business, advertising and marketing practices. (para.3)*
- *Businesses should not make any representation or omission or engage in any practice that is likely to be deceptive, misleading, fraudulent or unfair. (para.4)*

The E-commerce Recommendation further provides that:

- *Businesses should not engage in deceptive practices related to the collection and use of consumers' personal data. (para.8)*
- *Businesses should comply with any express or implied representations they make about their adherence to industry self-regulatory codes or programmes, privacy notices or any other policies or practices relating to their transactions with consumers. (para.11)*

Furthermore, the E-commerce Recommendation also addresses conduct by third parties, providing that:

- *Businesses should not permit others acting on their behalf to engage in deceptive, misleading, fraudulent or unfair practices and should take steps to prevent such conduct. (para.9)*

Annex B. Application of consumer protection laws to non-monetary transactions

Following consumers' increasing use of "free" goods and services in exchange for consumer data, the E-commerce Recommendation now explicitly includes non-monetary transactions in its scope. Non-monetary transactions often involve digital content products, including software, apps, videos, music, images, e-books, cloud computing, and social networking services. Non-monetary transactions can be part of more complex arrangements in which a basic service is provided free of charge, but "premium" versions with additional features are also offered against a payment ("freemium" models).

In some jurisdictions, consumer authorities have long applied prohibitions against deceptive business conduct to non-monetary transactions. There have also been recent developments in the application of consumer protection laws to non-monetary transactions in other jurisdictions. For example, the EC's proposal for a *Directive on certain aspects concerning contracts for the supply of digital content* provides consumers with the same remedies vis-à-vis defective digital products, irrespective of whether the consumer provides a monetary payment or consumer data (European Union, 2015[48]). The Directive would however not apply where consumer data is exclusively processed by the trader for supplying digital content, or for the trader to comply with legal requirements to which it is subject, and where the trader does not process the data for any other purpose. The EC's proposed New Deal for Consumers entails new consumer rights for digital services acquired without monetary payment. The proposal will extend the 14-day withdrawal rights applying to digital products purchased with money to digital services acquired in exchange for consumer data (EC, 2018[49]).

There have also been key legal rulings in relation to applying consumer protection to non-monetary transactions. One example is a decision made in 2018 by the Paris Tribunal, in a case brought by the French Consumers' Association against Twitter. The decision highlights that consumer protection law can be applied to a social media service's terms and conditions even if consumers do not pay money for the services. The Tribunal decided that Twitter users are consumers and that consumer protection law applies to those transactions where consumer data and other data are provided in exchange for the services (Paris Tribunal, 2018[50]). Similar positions on the application of consumer protection laws to non-monetary transactions have been taken by the French Competition Authority in relation to services offered by Google and Facebook (L'Autorité de la concurrence, 2018[51]) and the Italian Competition Authority against Facebook (AGCM, 2018[32]).

It should be noted that references to non-monetary transactions in this guide do not include the provision of goods or services without an explicit contractual agreement or registration process between businesses and consumers. Therefore, this guide does not cover the provision of so-called "free" services where consumers are not required to conclude a contract and provide consumer data in return for the service. Although it is out of the scope of the paper, it should be noted that some of the practices where there is no contract or registration might still be relevant to the E-commerce Recommendation. For instance, if a business makes a deceptive representation about data tracking on a free news website that does not require registration, this practice may still contravene in some cases fair business provisions under the E-commerce Recommendation.

References

ACCC (2019), *Digital Platforms Inquiry: final report*, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf. [43]

ACCC (2019), *HealthEngine in court for allegedly misusing patient data and manipulating reviews*, https://www.accc.gov.au/media-release/healthengine-in-court-for-allegedly-misusing-patient-data-and-manipulating-reviews. [26]

AGCM (2018), *Facebook fined 10 million Euros by the ICA for unfair commercial practices for using its subscribers' data for commercial purposes*, http://en.agcm.it/en/media/press-releases/2018/12/Facebook-fined-10-million-Euros-by-the-ICA-for-unfair-commercial-practices-for-using-its-subscribers%E2%80%99-data-for-commercial-purposes (accessed on 28 February 2019). [32]

AGCM (2017), *Decision no. 26597 – PS10601 Whatsapp-Trasferimento dati a Facebook*, http://www.agcm.it/dotcmsDOC/allegati-news/PS10601_scorrsanz_omi.pdf (accessed on 27 February 2019). [31]

Authority for Consumers and Markets (Netherlands) (2019), *ACM takes lead in international call on Apple and Google about app stores*, https://www.acm.nl/en/publications/acm-takes-lead-international-call-apple-and-google-about-app-stores. [36]

Competition Bureau Canada (2018), *Big data and innovation: key themes for competition policy in Canada - Competition Bureau Canada*, https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04304.html (accessed on 15 January 2019). [12]

Competition Bureau Canada (2017), *Big data and Innovation: Implications for Competition Policy in Canada*, https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/Big-Data-e.pdf/$file/Big-Data-e.pdf (accessed on 26 September 2018). [11]

Consumer Policy Research Centre (2019), *A Day in the Life of Data Removing the opacity surrounding the data collection, sharing and use environment in Australia*, http://www.cprc.org.au. (accessed on 26 June 2019). [4]

EC (2019), *Facebook changes its terms and clarify its use of data for consumers following discussions with the European Commission and consumer authorities*, http://europa.eu/rapid/press-release_IP-19-2048_en.htm (accessed on 25 June 2019). [34]

EC (2018), *A New Deal for Consumers: Commission strengthens EU consumer rights and enforcement*, http://europa.eu/rapid/press-release_IP-18-3041_en.htm (accessed on 19 October 2018). [49]

EC (2018), *Facebook, Google and Twitter accept to change their terms of services to make them customer-friendly and compliant with EU rules*, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=614254 (accessed on 28 September 2018). [47]

EC (2017), *The European Commission and Member States consumer authorities ask social media companies to comply with EU consumer rules*, http://europa.eu/rapid/press-release_IP-17-631_en.htm (accessed on 1 March 2019). [33]

EC (2016), *Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices*, http://dx.doi.org/10.1509/jmr.11.0467. [39]

European Parliament (n.d.), *EU Directive on Unfair Commercial Practices*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0029 (accessed on 19 June 2019). [41]

European Union (2015), *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of digital content*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015PC0634 (accessed on 1 March 2019). [48]

GVH (2018), *Competition Proceeding against Google is closed with Commitment Decision*, http://www.gvh.hu (accessed on 28 September 2018). [29]

Helberger, N., F. Borgesius and A. Reyna (2017), "The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law", *Common Market Law Review*, Vol. 54/5, pp. 1427-1465, https://www.kluwerlawonline.com/abstract.php?area=Journals&id=COLA2017118# (accessed on 19 October 2018). [22]

ICDPPC (2018), *ICDPPC Digital Citizen and Consumer Working Group: Report to the 40th Conference on the collaboration between Data Protection, Consumer Protection and other Authorities for Better Protection of Citizens and Consumers in the Digital Economy*, https://icdppc.org/wp-content/uploads/2018/11/ICDPPC-DCCWG-Report-Final.pdf (accessed on 24 June 2019). [7]

ICPEN (2018), *Joint Open Letter to Businesses in the Digital Economy on the Importance of Standard Terms and Conditions for Consumers*, https://www.icpen.org/news/902 (accessed on 18 March 2019). [35]

Italian Competition Authority (2017), *WhatsApp fined for 3 million euro for having forced its users to share their personal data with Facebook*, http://www.agcm.it/en/newsroom/press-releases/2380-whatsapp-fined-for-3-million-euro-for-having-forced-its-users-to-share-their-personal-data-with-facebook.html (accessed on 7 September 2018). [21]

L'Autorité de la concurrence (2018), *Avis n° 18-A-03 du 6 mars 2018 portant sur l'exploitation des données dans le secteur de la publicité sur internet*, http://www.autoritedelaconcurrence.fr/pdf/avis/18a03.pdf (accessed on 28 February 2019). [51]

Norway Consumer Authority (2019), *Calling on Apple and Google to improve information on personal data in their app stores*, https://www.forbrukertilsynet.no/eng-articles/calling-apple-google-improve-information-personal-data-app-stores (accessed on 18 March 2019). [37]

Norwegian Consumer Council (2016), *Happn shares user data in violation of its own terms*, https://www.forbrukerradet.no/side/happn-shares-user-data-in-violation-of-its-own-terms/ (accessed on 16 October 2018). [14]

Norwegian Consumer Council (2016), *Runkeeper must do more to earn users' trust*, https://www.forbrukerradet.no/uncategorized/runkeeper-must-do-more-to-earn-users-trust/ (accessed on 27 September 2018). [25]

Norwegian Consumer Council (2016), *Runkeeper tracks users when the app is not in use*, https://www.forbrukerradet.no/side/runkeeper-tracks-users-when-the-app-is-not-in-use/ (accessed on 27 September 2018). [24]

OECD (2019), *Challenges to Consumer Policy in the Digital Age*, http://www.oecd.org/sti/consumer/challenges-to-consumer-policy-in-the-digital-age.pdf. [3]

OECD (2019), *Online Advertising: Trends, Benefits and Risks for Consumers*, http://www.oecd.org/going-digital. (accessed on 14 January 2019). [42]

OECD (2019), *Summary of Roundtable on Digital Assistants and Voice-Controlled e-commerce*, https://one.oecd.org/document/DSTI/CP(2019)10/FINAL/en/pdf. [2]

OECD (2018), *Consumer Policy and the Smart Home*, https://www.oecd-ilibrary.org/docserver/e124c34a-en.pdf?expires=1550767955&id=id&accname=guest&checksum=260813946C789A999616079FF8E619EF (accessed on 4 March 2019). [1]

OECD (2018), *Toolkit for Protecting Digital Consumers: A Resource for G20 Policy Makers*, https://www.oecd.org/sti/consumer/toolkit-for-protecting-digital-consumers.pdf (accessed on 3 October 2018). [5]

OECD (2016), "Recommendation of the Council on Consumer Protection in E-commerce", http://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf (accessed on 14 August 2017). [8]

OECD (2013), "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", *OECD Digital Economy Papers*, No. 220, OECD Publishing, Paris, https://dx.doi.org/10.1787/5k486qtxldmq-en. [9]

OECD (2013), *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (accessed on 23 August 2018). [6]

Office of the Privacy Commissioner of Canada (2016), *Ashley Madison Investigation — Takeaways for all Organizations*, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/issue-specific-guidance-for-businesses/2016_005_ta/ (accessed on 27 February 2019). [27]

Paris Tribunal (2018), *the Decision of the Tribunal on the Case against Twitter*, http://entreprises.claisse-associes.com/wp-content/uploads/2018/08/TGI-Paris-7-ao%C3%BBt-2018-UFC-Twitter.pdf (accessed on 2 October 2018). [50]

PROFECO (2019), *Communications with the Secretariat*. [38]

UK CMA (2018), *Online dating services*, https://www.gov.uk/cma-cases/online-dating-services#case-closed (accessed on 27 February 2019). [30]

UK CMA (2015), *The commercial use of consumer data*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf (accessed on 26 February 2019). [13]

US FTC (2019), *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions. [17]

US FTC (2019), *FTC Sues Cambridge Analytica, Settles with Former CEO and App Developer*, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer. [20]

US FTC (2018), *California Company Settles FTC Charges Related to Privacy Shield Participation*, https://www.ftc.gov/news-events/press-releases/2018/07/california-company-settles-ftc-charges-related-privacy-shield (accessed on 28 February 2019). [19]

US FTC (2018), *Federal Trade Commission Gives Final Approval to Settlement with Uber*, https://www.ftc.gov/news-events/press-releases/2018/10/federal-trade-commission-gives-final-approval-settlement-uber (accessed on 28 February 2019). [16]

US FTC (2017), *FTC Approves Final Consent Order with Online Company Charged with Deceptively Tracking Consumers Online and Through Mobile Devices*, https://www.ftc.gov/news-events/press-releases/2017/04/ftc-approves-final-consent-order-online-company-charged (accessed on 27 February 2019). [18]

US FTC (2017), *Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims*, https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data (accessed on 28 February 2019). [15]

US FTC (2017), *VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent*, https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it (accessed on 28 February 2019). [23]

US FTC (2016), *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues*, https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf (accessed on 27 September 2018). [10]

US FTC (2016), *Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers*, https://www.ftc.gov/news-events/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive (accessed on 28 February 2019). [46]

US FTC (2016), *Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information*, https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting (accessed on 18 March 2019). [28]

US FTC (2015), *Built to Last: Section 5 and the Changing Marketplace; speech by Jessica Rich Director, Bureau of Consumer Protection, FTC*, https://www.ftc.gov/system/files/documents/public_statements/626841/150226section5symposium.pdf (accessed on 28 February 2019). [44]

US FTC (2014), *FTC Charges Data Broker with Facilitating the Theft of Millions of Dollars from Consumers' Accounts*, https://www.ftc.gov/news-events/press-releases/2014/12/ftc-charges-data-broker-facilitating-theft-millions-dollars (accessed on 28 February 2019). [45]

vzbv (2018), *Facebook in Breach of German Data Protection Law*, https://www.vzbv.de/sites/default/files/downloads/2018/02/14/18-02-12_vzbv_pm_facebook-urteil_en.pdf (accessed on 28 September 2018). [40]