Policies and Tools for Improving Digital Economy and Competition in Digital Markets: Current Issues

APEC Digital Economy Steering Group
and Competition Policy and Law Group

March 2024

Asia-Pacific
Economic Cooperation

Asia-Pacific
Economic Cooperation

Policies and Tools for Improving Digital Economy and Competition in Digital Markets: Current Issues

APEC Digital Economy Steering Group
and Competition Policy and Law Group

March 2024

APEC Project: DESG 03 2022A

Produced by

The Federal Telecommunications Institute (IFT)
Insurgentes Sur 1143, Col. Nochebuena,
Benito Juárez, Mexico City, 03720.
Tel: +52 55 5015 4000
Email: asuntosinternacionales@ift.org.mx
Website: https://www.ift.org.mx/

In collaboration with the Federal Economic Competition Commission (COFECE)
Av. Revolución 725, Col. Santa María Nonoalco,
Benito Juárez, Mexico City, 03700.
Tel. +52 55 2789 6500
Email: international@cofece.mx
Website: https://www.cofece.mx/

For
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

APEC#224-CT-01.8

Table of Contents

Policies and Tools for Improving Digital Economy and Competition in Digital Markets: Current Issues[1]

1 Introduction

Digital platforms provide a variety of services for many different users, individuals or firms that seek information, entertainment, transactions and social interactions, as buyers, sellers, software producers and users, ancillary service providers and so on. Some digital market participants can play a dual role of being simultaneously operators for the platform and sellers of their own products and services in competition with other rival sellers. Furthermore, digital platforms have the ability to bundle a range of digital services into a seamless data-driven offer that enables them to expand into adjacent markets.

Competition research on digital markets has stressed the importance of certain economic features which influence and determine competition processes and dynamics, which in turn affect consumer's welfare and economic prosperity. Some of the most relevant features are: direct network effects, indirect network effects, economies of scale and scope,[2] and data-driven network effects. In some cases, these features combined with consumer inertia (tendency to single-home) and high switching costs (e.g. changing between providers can be costly for consumers due to strong direct network effects), can produce lock-in effects for consumers.[3] These features could act as barriers to entry that potentially could make them highly concentrated, prone to tipping, and not easily contestable in certain jurisdictions. In those cases, this could lead to some firms having the ability and incentives to pose risks to consumers' welfare (or to jeopardize the adequate protection of their rights'), as well as markets' contestability, performance, and innovation.[4]

In dealing with these issues, APEC economies could benefit from understanding how regulatory approaches, as well as antitrust enforcement tools can enhance one another. Since, on the one hand, interventions that promote competition can empower consumers, reduce incentives to single-homing, and foster innovation; and, on the other, regulations can give consumers more confidence to engage with new entrants by effectively enforcing safeguards and protections, and could even promote innovation.

Hence, authorities in the APEC region have been recently discussing what mix of competition and regulatory policies and tools are needed to tackle concerns regarding:

- Consumers' protection: intersection between Consumer Protection in Digital Markets and Competition Enforcement;
- Online safety, regulatory and competition issues; and

[1] This Report, researched and written under the direction of the Federal Telecommunication Institute (IFT), in collaboration with the Federal Economic Competition Commission (COFECE) of Mexico, represents Mexico's best understanding of developments and issues relevant to the topics addressed in the report "Policies and Tools for Improving Digital Economy and Competition in Digital Markets. Economies: Current Issues". Readers are advised to review the latest version of the cases and the best practices presented in this report, due to their novelty changes might have occurred since its latest revision in December 2023. This Report does not purport to be representative of the thinking or consensus of the APEC CPLG or DESG or their individual members or the speakers at its Workshop.

[2] APEC (2019). *Competition Policy for Regulating Online Platforms in the APEC Region*, pp. 13-17. Available at: https://aimp2.apec.org/sites/PDB/Supporting%20Docs/3732/Completion%20Report/CPLG%2002%2018%20Project%20Report.pdf.

[3] UNCTAD (2020). *Strengthening consumer protection and competition in the digital economy*, p. 10. Available at: https://unctad.org/system/files/official-document/tdrbpconf9d4_en.pdf.

[4] In some jurisdictions some digital platforms have been found to hold market power across different digital markets, and even in some jurisdictions they have been subject to specific regulations.

- Collaboration between competition and regulatory authorities to tackle harms and risks from data collection and analysis.

2 Insights from Virtual Sessions

In the following section it is presented a summary of the most important points addressed during the virtual sessions.

2.1 Virtual Session 1: "Consumers' protection: interplay between Consumer Protection and Competition Enforcement in Digital Markets —Artificial intelligence and Dark Patterns—"

The opening remarks were delivered by Javier Juárez Mojica, acting Chairman of Mexico's Federal Telecommunications Institute (IFT), and Andrea Marván Saltiel, Chairwoman of Mexico's Federal Economic Competition Commission (COFECE). The opening remarks highlighted the roles that IFT and COFECE play in the development of the digital ecosystem in Mexico, the challenges in regulating business models based on digital markets and the importance of international cooperation, information and experiences sharing and identifying regional synergies to face the digital transformation in the design of policies and regulations that tackle challenges and emerging issues in the digital economy.

Keynote Speaker: Professor Alexandre de Streel, Academic Director of the Digital Research Program at College of Europe, Center of Regulation in Europe.

Professor de Streel intervention explained the general terms of the Digital Platforms Regulatory Framework from the European Union (EU) which includes the Digital Markets Act (DMA) and Digital Services Act (DSA). He explained that the new regulatory framework was considered necessary to address competition, consumers and democratic concerns. In particular, the uncontestable market position of a few digital platforms has been leading to unfair market results, loss of autonomy of citizens, business users and the Member States of the EU. In this sense, the DMA aims to improve market contestability and innovation (intra-platform competition, inter-platform competition, and diagonal competition); and fairness (*ex ante* to level the playing field and ex post redistributive). Hence, the DMA includes the following clauses to regulate digital gatekeepers: transparency in ad intermediation; prevention of anti-competitive leverage (tying, discrimination and self-preferencing); facilitate switching and multi-homing; access to platforms and data, among others. Regarding the DSA, Professor de Streel explained that it is a Risk based regulation, which imposes more obligations when risks are higher; more harmful content; and weaker recipients (e.g. children). In this sense, he highlighted the European Union's experience in protecting users while also maximizing the opportunities the digital platforms are offering and minimizing the risks.

Keynote Speaker: Professor Ariel Ezrachi, Slaughter and May Professor of Competition Law, Director of the Centre for Competition Law and Policy, University of Oxford.

Professor Ezrachi's intervention addressed the economic and enforcement choices that have been implemented in the European Union. Considering this, he emphasized that competition authorities should analyze the aggregated effect of the following features of digital markets: network effects (direct and indirect); data as critical input; advanced analytics (algorithms & AI) and data collection; asymmetry of information and analytical power; key gate keepers, sustained market power, stealth (capabilities of tracking, harvesting, targeting and manipulation); winner takes all (due to persistence, scale, data, networks), and economies of scale and scope, among others. To address them, he explained the different choices available to authorities which include regulatory policies and enforcement methods and tools. However, he noticed that there are challenges in applying

them, such as the adequate level of intervention —What actions and strategies should be supported and which condemned?, such as the risk of chilling effect on innovation and investment; types of business models and value chains—. Accordingly, he recommended that authorities should focus on the main concerns: (i) collusion –pricing algorithms, hub and spoke and the role of artificial intelligence; (ii) manipulation of consumers –targeting and manipulations (dark patterns); (iii) market power and the role of digital ecosystems in the competitive dynamics and innovation. He explained and gave examples on each one of them. Finally, he concluded that the asymmetry of power and capabilities of certain digital providers, requires enforcers to increase in-house capacity and expertise; the increased centrality of online markets, new technologies, and new business models, require recalibration of enforcement efforts; and the need for measured, collaborative intervention among competition and other authorities.

APEC expert from The United States: Michael D. Panzera, Counsel for International Consumer Protection and Privacy, Office of International Affairs, Federal Trade Commission (FTC).

In his presentation, he explained the role of the FTC and provided an update on the agency's latest activities related to artificial intelligence and consumer data. In particular, he outlined several concerns regarding artificial intelligence that have been identified by the FTC, including: improper use of personal data; the ability to evade security safeguards; uncertainties regarding liability for consumer harms; the potential for biased or unfair decisions; power asymmetries between consumers and companies; and enhanced price discrimination. To address concerns related to artificial intelligence and consumer data, the FTC has may take action pursuant to Section 5 of the FTC Act, the Fair Credit Reporting Act, and the Equal Credit Opportunity Act, among other statutes. Also, he gave an overview of the objectives of the 2022 Advanced Notice of Proposed Rulemaking (ANPR) on "Commercial Surveillance and Data Security", which will address: (i) how companies collect, aggregate, protect, use, analyze, and retain consumer data; (ii) how companies transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive.

APEC expert from Australia: Georgia MacKenzie, Assistant Director, Digital Platforms Branch, Australian Competition Consumer Commission (ACCC).

In her presentation she described the Australian perspectives on dark patterns and their impact on consumers. According to the ACCC, dark patterns refer to the design of user interfaces intended to confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions. She provided some examples of the ACCC's findings on dark patterns used by digital platforms. The current Australian Consumer Law prohibits misleading or deceptive conduct in trade or commerce, and false or misleading representations about goods or services. Certain dark patterns are prohibited under these laws. However, not all dark patterns are false, misleading or deceptive which means they are not prohibited, despite distorting or undermining consumer choice The ACCC considers Australia's competition and consumer protection laws are not sufficient in the digital context, so it has recommended that the Australian Government implement a range of new measures to address harms from digital platforms. In particular, the ACCC recommended that there should be an economy-wide prohibition on unfair trading practices, including harmful dark patterns. The ACCC also recommended that there should be service-specific codes of conduct for designated digital platforms, setting out targeted competition

obligations (which could include, for example, a ban on anti-competitive dark patterns that frustrate consumer switching).

APEC expert from Canada: Orla Bartolo, Assistant Deputy Commissioner of the Digital Enforcement Directorate, Competition Bureau Canada (CBC).

In her presentation she provided insights on how the CBC is innovating by introducing new expertise and what the Canadian government is doing to modernize its legislative portfolio. The CBC's new Digital Enforcement and Intelligence Branch is driving thinking and understanding of competition issues around artificial intelligence and other emerging technologies. Ms. Bartolo explained the introduction of new capabilities will enhance the CBC's enforcement and advocacy work, will drive a proactive approach to find and stop harm to competitive markets, and ultimately will reduce the gap between the pace in markets and the CBC's work. In Canada, establishing a balance between enforcement and regulation without stifling innovation has a significant focus. In 2023, the Canadian Digital Regulators Forum was established by CBC, the Office of the Privacy Commissioner of Canada, and the Canadian Radio-Television and Telecommunications Commission.[5] Its purpose is for its members to strengthen information sharing and collaboration on topics that relate to digital markets or platforms. It is an informal means, where members may exchange best practices, conduct research, market analysis, and problem solve. Ms. Bartolo highlighted legislative amendments that identify drip pricing as a misleading business practice. She also spoke of the 2023 Fraud Prevention Month theme that provided Canadians with tips and tricks to recognize conduct used to entrap victims, such as dark patterns. Lastly, she spoke of legislative changes in Canada to increase responsiveness and agility when it comes to keeping pace with technology and digital markets. This includes the modernization of the *Competition Act*. More broadly other relevant digital legislative developments in Canada include: the *Online Streaming Act,* the *Online News Act*, the *Digital Charter Implementation Act*. The last of which, introduces three proposed acts and makes consequential and related amendments to other Acts to strengthen Canada's private sector privacy law and creates new rules for responsible development and deployment of AI.

2.2 Virtual Session 2: "Online Safety, regulatory and competition issues"

Keynote Speaker: Will Pinkney, Principal, Networks and Communications, Office of Communications (OFCOM), United Kingdom.

Mr. Pinkney explained that the United Kingdom's (UK) government is establishing new forms of regulation in response to the challenges posed by digital markets. Firstly, he explained that the government proposed the Online Safety Bill to ensure that the regulated services have effective systems in place to keep people safe online. Hence, among the main requirements for firms will include having risk assessment and transparency processes and offering users simple ways to report issues and seek redress. The regime will focus on illegal offences (terrorism-related material, the sale or supply of restricted items, and online fraud) and child protection. Secondly, he explained that the Competition and Markets Authority (CMA) established a Digital Markets Unit which will oversee a new pro-competitive regulatory regime. This new regulatory regime will apply to the most powerful digital firms, preventing them from using their market positions to limit innovation or market access. In this regard, the CMA and OFCOM have published a joint statement that explain some of the interactions between competition and online safety, and how they

[5] Canada-Government of Canada (2023). *Canadian Digital Regulators Forum*. Available at: https://ised-isde.canada.ca/site/competition-bureau-canada/en/how-we-foster-competition/collaboration-and-partnerships/canadian-digital-regulators-forum.

expect to work together in order to avoid unintended consequences from both regimes. Thirdly, he explained that while competition can improve online safety by increasing options and innovations available to consumers, there is a risk that the online safety regime might increase market entry costs and competition interventions may worsen online safety outcomes if they prevent companies from taking necessary action to protect users. For example, some have voiced concerns that pro-competition interoperability requirements might affect their ability to maintain online safety. Finally, he recognized that CMA and OFCOM will need to continue to work together to identify where the interactions between the two regulatory frameworks may arise, in order to collaborate when they do, to deliver the best outcomes for internet users in the UK.

Keynote Speaker: John Newman, Deputy Director, Bureau of Competition, FTC, The United States.

Mr. Newman explained where the different sources of digital power come from. In particular, he explained the role of: switching costs, differentiation, and network effects. Regarding the latter, he explained how different types of network effects can combine and lead to a base of "sticky" trading partners which can make difficult to other providers to challenge the market power of an incumbent player. Also, he explained that some digital platforms with market power behave as "thick" intermediators, because they intermediate many of the interactions that occur between different groups of users of the platforms. Considering these two, Mr. Newman explained how competition authorities can better address challenges from digital platforms, such as: (i) reduce gaps of imperfect information: require most relevant information for merger analysis, increase sources of knowledge coming from other expertise areas (technologists, behavioral economists, sociologists, etc.), wider range of direct evidence of power (less privacy, more ads, payments, etc.); and (ii) establishing guidelines to improve enforcement actions: establishing thresholds from different variables and prefer structural solutions when dealing with thick intermediaries, to avoid the exploitation of walkarounds. Finally, he addressed what is the role of competition in promoting online safety, in this regard he explained that competition authorities should promote fair competition, to promote better outcomes for consumers, and enhance coordination between competition and consumer protection authorities to better deal with online protection for consumers.

APEC expert from Australia: **Madeleine Houghton**, Assistant Director, Digital Platforms Branch, Australian Competition Consumer Commission (ACCC).

She explained that consumer protection and privacy are common online safety issues that intersect with competition law and policy. The ACCC promotes a holistic approach to address intersecting issues of data protection, competition and consumer protection in digital markets through: enforcement matters, market studies (and resulting recommendations), and inter-agency engagement. In the case of enforcement, she explained that in the Google/Double Click case, the ACCC alleged that Google had engaged in misleading or deceptive conduct when it published an on-screen notification to Australian users and changed its privacy policy to expand the scope of its use and collection of personal data. In the case, the ACCC focused on theories of harm related to consumers' privacy. In the fifth report of the Digital Platform Services Inquiry, the ACCC has recommended a new regulatory framework that considers competition and consumer harms (including privacy related harms) which the ACCC has observed in the supply of digital platform services. These recommendations are currently being considered by the Australian

Government. Also, she explained that the ACCC is working along with the Australian Communications and Media Authority, the Office of the Australian Information Commissioner (Australia's privacy regulator) and the Office of the eSafety Commissioner, as part of Australia's Digital Platforms Regulators Forum (DP-Reg) on issues of intersection between competition, consumer, privacy, and online safety.

APEC expert from Mexico: **Desiree Delgado Arcos**, Director of Market Analysis, Competition Unit, Federal Telecommunications Institute (IFT).

She presented the legal duties of the IFT, as a competition and regulatory body for the Telecommunications and Broadcasting sectors in Mexico, as well as the duties of other public and regulatory authorities relevant in the broadcasting sector. She explained how the audiovisual content market has changed in the last years, as well as three factors that have contributed to changes in the competitive dynamics: technological evolution (algorithms and data analytics); the rise of new digital players (OTTs, users providing their own content, etc.); as well as the creation of the Ad Tech industry, and she noted how these changes affected not only dynamics but also incentives of online players to tackle online safety issues. In this sense, she addressed how these new factors can lead to potential threats to online safety, such as: low cost of disseminating harmful (illegal) content; recommendation algorithms can increase the reach and dissemination of content that despite being popular with users, it may lead to harms; the economic aspects of digital platforms can play a crucial role in leading to market tipping and big digital players' market power in online advertising and other markets. Hence, she asserted that policy interventions should address harms that can result from market power and broad online safety risks. She stressed that it's therefore very important that regulators have access to different toolkits: one to address harms that can result from market power; and another to address online safety risks. Finally, she explained some of the actions that have been taken by the IFT.

2.3 Virtual Session 3: "Collaboration between Competition and Regulatory Authorities to Tackle Harms and Risks from Data Collection and Analysis"

Keynote Speaker: Miriam Stankovich, Principal Digital Policy Specialist, Center for Digital Acceleration (DAI).

She explained some of the core data protection principles core of several privacy regulation frameworks, and that data protection also interacts with other regulatory frameworks: cybersecurity, competition, consumer protection, and other specific sectors (health, finance, etc.). Also, she explained that there are many different approaches to regulate data protection (horizontal approach vs specific sectoral regulations), but she warned there are many economies that still do not have a regulatory framework for data protection. Most regulatory frameworks distinguish between owners, aggregators and controllers of data, however there are no universal definitions for them, which can be challenging these players. Also, regulators have to consider what type of data is being collected, how data is being used and for what purposes. Hence, regulators need to consider how data collection and use can lead to market power imbalances & information asymmetries between firms. In such a case, regulators need to consider: (i) economies of scope, (ii) causes of fragmentation and (iii) how the combination of economies of scope and scale work, such as many digital markets are two-sided—provide services to vendors & other supply-chain companies and provide sales and services to end users (web of transactions and terms and conditions open up dangers of anti-competitive behavior).

Keynote Speaker: Daniel Schnurr, Chair of Machine Learning and Uncertainty Quantification, University of Regensburg & Centre on Regulation in Europe.

Dr. Schnurr presented an overview of the empirical evidence on data-driven business value. In particular, it explained that data can be used for targeted advertising, recommendation systems and service personalization, these three uses of data can be used by the biggest digital platforms to sustain a competitive advantage. In particular, digital platforms can use the following practices to sustain such advantage: exclusive data access; increase switching costs by using data; exploitative data access (reducing privacy options for consumers); network effects and ecosystems, all of which can enhance digital market power. Accordingly, competition authorities could analyze data-driven theories of harm, such as: lack of contestability in established markets; lack of contestability in new or emerging markets (domino effect, envelopment and unlevelled playing field); reduction of downstream competition (vertical integration, self-preferencing, and margin squeeze); data agglomeration from 'ancillary' data services (payment and identification services). Also, theories of harm to innovation, such as: lower innovation in 'tipped' markets (less competitive pressure and killer acquisitions); lower innovation in 'related' markets (leverage of market power in adjacent markets); unduly efficiencies from integration and economies of scope and scale in data. To address harms from extensive data collection, authorities might carefully consider the following: data as a by-product vs. data as a main product, existence of viable commercial offers (actual competitors); technologies for anonymization that are privacy-enhancing, data trusts and data sandboxing, and unlawfulness of de-anonymization.

APEC expert from Australia: Holly Ritson, Assistant Director, Digital Platforms Branch, ACCC.

She described the market inquiries relating to digital platforms and data that the ACCC has undertaken, including the Digital Platforms Inquiry (2017-2019) (DPI), the Advertising Technology Services Inquiry (2020-2021), and the Digital Platform Services Inquiry (2020-2025) (DPSI). She explained that in the DPI, the ACCC found that collection of user data is central to the business model of advertiser-funded platforms, and the biggest digital platforms, such as Meta and Google, have a strong competitive advantage due to the breadth and depth of user data they collect —they have multiple touch points that allow them to collect more and higher quality user data. In the Digital Advertising Services Inquiry (2020-2021), the ACCC found that Google dominates the supply of ad tech services in Australia, and in particular, found that Google's access to data (a "data advantage") has contributed to its dominance. To address Google's data advantage, the ACCC recommended it be given the power to implement measures including: (i) data separation measures and (ii) data access requirements. Finally, she explained that as part of the DPSI, the ACCC is conducting market studies on the following topics: Expanding Ecosystems (forthcoming late 2023) and Data Brokers (forthcoming early 2024). Regarding the first, the ACCC is exploring the role of data in digital platforms' expansion strategies, including the extent to which platforms use data across their ecosystems, and the impact of this on platforms' competitive position. In the latter the ACCC will consider competition and consumer considerations regarding how data brokers provide access to data to participants in the digital economy and how data brokers compete in Australia.

APEC expert from Mexico: Lizeth Martínez Nagore, Executive Director at the General Directorate of Mergers Federal Economic Competition Commission (COFECE).

She explained the main elements analyzed in the Walmart/Cornershop and Uber/Cornershop mergers. Regarding the first, she explained the main theories of harm considered by the COFECE, such as: (i) Cornershop could refuse to offer its services to Walmart competitors; (ii) Walmart could refuse to retail its products on platforms operated by Cornershop's competitors; and (iii) the new merged entity could induce Walmart's competitors to exit the Cornershop platform through the strategic use of information produced and provided by competitors to retail their products. COFECE blocked the proposed merger since it proved it would distort competition in the market of logistical services for the exhibition, purchase and immediate delivery of products sold by supermarkets and membership price clubs through websites and mobiles apps to final consumers. Regarding the second, the main theories of harm identified by the authority were: loss of potential competition in logistical services for the exhibition, purchase and delivery of products sold by retailers through mobile apps and websites to final consumers (grocery's delivery service); elimination of innovation: the elimination or loss of potential competition would originate the elimination of innovation; creation of a larger ecosystem and a single sign on platform that competitors may find hard to replicate this may end with the exit of some competitors or aboding new entrants. The merger was cleared since the authority did not find any foreclosure strategy to be profitable.

APEC expert from Japan: Satoshi Yoshida, Deputy Director, Office of Policy Planning and Research for Digital Markets, Japan Fair Trade Commission (JFTC).

In his presentation, first, he gave an overview of the Japanese Government Authorities' activities on data collection, showing related activities of the Ministry of Internal Affairs and Communications, the Personal Information Protection Commission, the Ministry of Economy, Trade and Industry and the Consumer Affairs Agency. He explained the objectives and main features of the "Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc.". In particular, he explained that it provides guide and clarification to digital providers on what constitutes "abuse of a superior bargaining position", and on the typical conducts that might fall under the abuses of a superior bargaining position over consumers regarding personal information gathering. He introduced some market studies of the JFTC which partially documented data collection issues. Finally, he gave an overview on the "Act on Improving Transparency and Fairness of Digital Platforms" which designates specific digital platform providers in certain categories and scales and it makes such providers subject to specific requirements such as disclosing trade terms and other information including those on data handling, and annually reporting to administrative authorities (the Ministry of Economy, Trade and Industry (METI)). Also, the Act requires METI to review the current situation of platform operation in accordance with the submitted yearly report, and authorizes METI's Minister to request the JFTC to take appropriate measures under the Antimonopoly Act if it is found that a designated digital platform provider may be suspected of being involved in any violation.

3 Policies and tools for improving digital economy and competition in digital markets: current issues

3.1 Consumers' protection: interplay between Consumer Protection and Competition Enforcement in Digital Markets –Artificial intelligence and Dark Patterns–

Online service providers usually may use data-powered algorithms to provide their services. For example, they can be used for the personalization of their services, such as recommendations (e.g. search queries, content recommendations, products, etc.) and dynamic optimization of their offers (e.g. dynamic pricing), among others. While the use of algorithms might increase the efficiency and revenues for digital providers, they could pose harms to consumers, such as: limiting their ability and capacity to make purchasing decisions, reducing their privacy and security, furthering anticompetitive practices that enhance or entrench the market power of dominant providers, which in turns affects consumer's welfare.

Also, online service providers usually use web pages and applications, collectively known as digital interfaces, to provide their services, presenting offers and options for contracts for their consumers. In the last couple of years, it has been documented by some authorities, that many online providers design their digital interfaces *"to manipulate a user's behavior and subvert a consumer's choices, causing the user to engage in conducts that they did not expect or desire, or impairing individuals' ability to make an informed decision."*[6,7]

Several economies are working to analyze how AI systems and the design of digital interfaces could limit the effectiveness of consumer protection, privacy, and competition policy in digital markets, and how can the collaboration between authorities improve the synergies and the consistency of their respective policy interventions.[8] Consequently, this section will address the following issues:

i. **Artificial Intelligence** (AI) and the use of automated systems for the personalization of services and prices.

ii. **Digital dark patterns**, harms for consumer's privacy, autonomy of consumer's decisions and competition.

For each of the previous issues, the following aspects will be discussed: (i) conceptual framework; (ii) benefits and risks; (iii) policies and regulations that have been or will be implemented in some economies; and (iv) how coordination and collaboration between authorities can enhance synergies and avoid unexpected consequences for consumers and competitive dynamics.

[6] Gesser, A., Skrzypczyk, J., Roberts M. R. and Muse, M. (2022). *"Dark Patterns: What Are They and How Can Companies Avoid Regulatory Scrutiny?"* From: Debevoise & Plimpton LLP, Blog. Available at: https://www.debevoisedatablog.com/2022/10/12/dark-patterns-what-are-they-and-how-can-companies-avoid-regulatory-scrutiny/.

[7] For example, digital interfaces could be strategically designed to limit the transparency of the terms of contracts they display; highlight options that benefit providers but not consumers; include subscriptions that, despite all efforts, seem impossible to cancel; terms and conditions hidden at the bottom of webpages; and buttons with confusing phrasing that result in an accidental agreement or purchase. United States of America-Congressional Research Service (2022). *What Hides in the Shadows: Deceptive Design of Dark Patterns*, p. 1. Available at: https://crsreports.congress.gov/product/pdf/IF/IF12246.

[8] OECD (2020). "Chapter 8. Consumer policy in the digital transformation". In *OECD Digital Economy Outlook 2020*. Available at: https://www.oecd-ilibrary.org/sites/7570fa4a-en/index.html?itemId=/content/component/7570fa4a-en.

3.1.1 Artificial Intelligence (AI)

3.1.1.1 General aspects and concerns

For the provision of online services, generative AI providers usually use a diverse set of inputs. First, as infrastructure elements they require: (i) data –unstructured and structured data–; (ii) high skilled labor; (iii) processing technologies –cloud computing services, graphical processing units, data warehouses, supercomputers, etc.–. Second, they require AI systems –algorithmic systems, e.g. machine learning (ML), deep learning algorithms, neural networks, natural language processing, etc.–. Third, to reach final consumers, they need: application programming interfaces (APIs) and digital interfaces: applications (apps) and webpages, etc.[9]

For the purposes of this document, AI systems[10] will be defined and grouped together as 'self-learning, adaptive systems'. There are various approaches to defining AI:[11]

- In terms of technologies, techniques and/or approaches: ML, deep learning, neural networks, generative AI, etc.[12]
- In terms of purpose: facial recognition, image recognition, natural language processing, etc.
- In terms of agents or machines: robots and self-driving cars, among others.

AI systems, and mainly ML, DL and NN, have been used strategically by big tech firms' in their ongoing operations for a while, for example Google's search and Facebook's News Feed.[13] Nowadays, some medium and small businesses, especially in developed economies, are increasingly using ML –property of third parties (i.e. as part of cloud computing services)–, in their business operations.[14] For example, Amazon Web Service Marketplace provides ML services for speech recognition, document summarization, among others.[15]

It has been estimated that the market for AI, for private and government applications, is expected to show strong growth in the coming decade. In 2021, its value was estimated in

[9] United Kingdom-Competition and Markets Authority (CMA). (2023). *AI Foundation Models: Initial review*. Available at: https://assets.publishing.service.gov.uk/media/64528e622f62220013a6a491/AI_Foundation_Models_-_Initial_review_.pdf; and Taddy, M. (2019). "Chapter 2: The Technological Elements of Artificial Intelligence", p. 61 and Varian, H. (2019). "Chapter 16: Artificial Intelligence, Economics, and Industrial Organization", p. 400. In: Agrawal, A., Gans, J. and Goldfarb, A. *The Economics of Artificial Intelligence: An Agenda*. University of Chicago Press. Available at: https://www.nber.org/books-and-chapters/economics-artificial-intelligence-agenda.

[10] AI systems work by combining many ML algorithms together –each targeting a straightforward prediction task– to solve complex problems. Hence, AI systems are self-training structures of ML predictors that automate and accelerate human tasks. As explained by M. Taddy (2019), machine learning is basically limited to predicting a future that looks mostly like the past, and is useful for pattern recognition. While, an AI system is able to solve complex problems that have been previously reserved for humans.

[11] International Telecommunications Union-ITU (2023). *Artificial intelligence for good*. Available at: https://www.itu.int/en/mediacentre/backgrounders/Pages/artificial-intelligence-for-good.aspx.

[12] Taddy (2019) explains that ML are algorithms that use past data to make predictions on future data and direct choices based on those predictions about specific tasks. AI systems are self-training structures of ML predictors, that make assumptions, test, learn, reiterate, etc., but that can do all these without human intervention. Also, AI systems can operate without ML, for example chatbots. Taddy, M. (2019). "Chapter 2: The Technological Elements of Artificial Intelligence", p. 61 and Varian, H. (2019). "Chapter 16: Artificial Intelligence, Economics, and Industrial Organization", p. 400. In: Agrawal, A., Gans, J. and Goldfarb, A. *The Economics of Artificial Intelligence: An Agenda*. University of Chicago Press. Available at: https://www.nber.org/books-and-chapters/economics-artificial-intelligence-agenda.

[13] For example, the use of generative AI, which can be used to influence people's beliefs, emotions, and behavior. See: FTC (2023). *The Luring Test: AI and the engineering of consumer trust*. Available at: https://www.ftc.gov/business-guidance/blog/2023/05/luring-test-ai-engineering-consumer-trust.

[14] United Kingdom-CMA (2021). *Algorithms: How they can reduce competition and harm consumers*. Available at: https://www.gov.uk/government/consultations/algorithms-competition-and-consumer-harm-call-for-information/algorithms-how-they-can-reduce-competition-and-harm-consumers#fn:3; webpage: https://www.gov.uk/government/consultations/algorithms-competition-and-consumer-harm-call-for-information/algorithms-how-they-can-reduce-competition-and-harm-consumers.

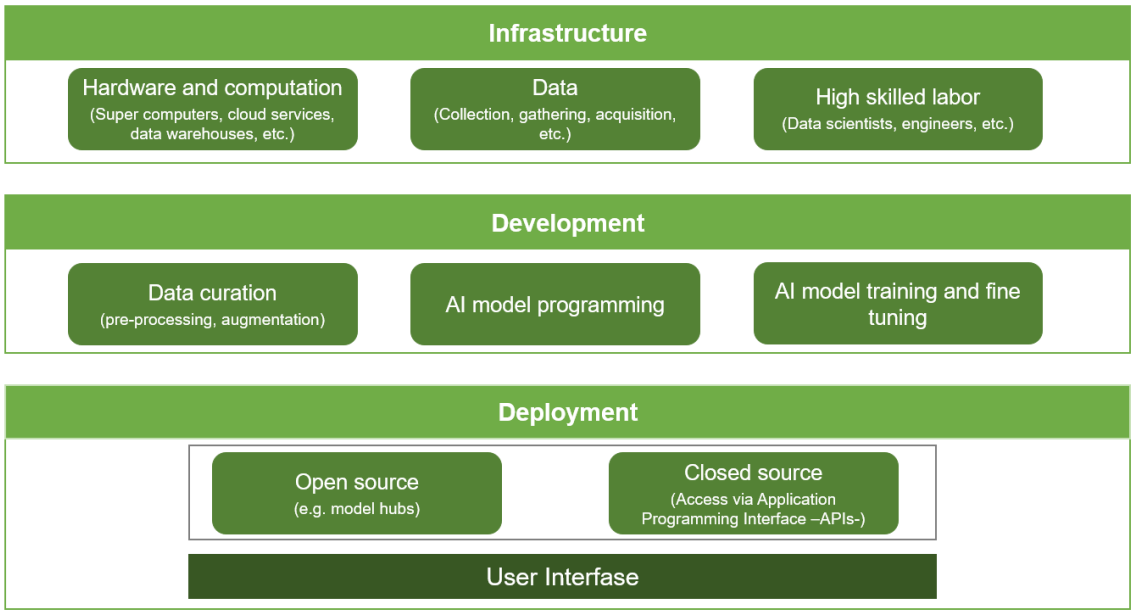
[15] Available at: https://aws.amazon.com/marketplace/.

nearly USD100 billion, and it is expected to grow twentyfold by 2030, up to nearly USD2 trillion.[16]

AI systems involve different actors responsible for the system's infrastructure, development and deployment. In some cases, one organization integrates all actors. In others, specialized companies provide access to an AI model through software or an application programming interface (API), without enabling direct interaction by a client. There are also others where one organization develops an AI model and another integrates that model into a company's software which is responsible of the direct interaction with the user.[17] The following figure shows how different actors participate in the provision of AI systems.

The following figure shows how digital providers could use different technologies and inputs to provide their services to final consumers.

Figure 1. Value chain of AI systems



Source: Own elaboration with information from CMA (2023) and De Silva and Alahakoon (2022).[18]

(For examples on how some sectors and industries are using AI systems, see Annex 1.)

As AI systems are more widely used by digital providers and become increasingly part of consumers' daily lives, academics, organizations, and governments have identified some general concerns regarding its use and implementation. The main concerns relate to: (i) transparency of the decision-making process; (ii) biases in the results and its implications for consumers; (iii) privacy and data gathering; and (iv) competition.

3.1.1.1.1 Economics of AI systems

This subsection will explain some of the economic characteristics that play a role in the investment and adoption of AI systems among digital providers.

[16] Next Move Strategy Consulting (2023). *Artificial Intelligence Market: Global Opportunity Analysis and Industry Forecast*. Available at: https://www.nextmsc.com/report/artificial-intelligence-market. According to the consultancy firm, the estimation includes investments of hardware, software and services, for the following applications: virtual assistants/chatbots, forecasting and modelling, text and speech analytics, computer vision, predictive maintenance, and others, for the following industries: governments, aerospace and defense, automotive, healthcare, IT and telecommunications, manufacturing, education, retail and e-commerce, energy and utilities media, etc.
[17] Engler, A.C. and Renda, A. *Reconciling the AI Value Chain with the EU Artificial Intelligence Act*, p. 3. Available at: https://cdn.ceps.eu/wp-content/uploads/2022/09/CEPS-In-depth-analysis-2022-03_Reconciling-the-AI-Value-Chain-with-the-EU-Artificial-Intelligence-Act.pdf.
[18] Adapted from United Kingdom-Competition and Markets Authority (CMA) (2023). p. 5. Op. Cit., and De Silva, D. and Alahakoon, D. (2022). "An artificial intelligence life cycle: From conception to production." *Patterns*, Volume 3, Issue 6, Available at: https://doi.org/10.1016/j.patter.2022.100489.

- **Economies of Scale from Data**: AI systems improve with the quantity and quality of data. (See section 4.3) Hence, *ceteris paribus*, companies that gather more and better data can generate more accurate predictions. As digital providers improve their services this tends to increase their customers base, which allows them to gather more data, which in turn generates more customers (direct network externalities). This positive feedback loop is what leads to economies of scale from data.[19] (See section 4.3)
- **Economies of Scale from developing AI Capabilities**: economies of scale also arise due to the high fixed costs of building and developing AI systems within a firm. In 2023, the cost of hardware and software required to build and develop proprietary AI systems is considered to be high by several experts, also the costs of acquiring data and the labor costs of high skilled workers do have an effect on the fixed and variable costs of firms, all of which lead to economies of scale as AI systems are more used within a firm.[20]

  Nonetheless, the costs of deploying an AI system to reach final consumers depends on the type of AI system required by a digital provider. For example, in the United States, in 2017 the cost to train an image recognition network, like ResNet-50, on a public cloud was approximately USD1,000; in 2019, the cost dropped approximately to USD10.[21] On the contrary, the costs of building, training and tuning novelty AI systems are on the rise. Brian Nowak of Morgan Stanley estimates that serving up an answer to a ChatGPT query costs roughly USD0.02, but about seven times more than the current AI system used for Google search queries because of the extra computing power required.[22] In this sense, more advanced and novel models require higher investments costs.
- **Vertical integration**. While some digital providers rely on third party AI systems (as well as data inputs and other infrastructures), few companies have the technical and financial capabilities to build and develop their own AI systems. Vertical integration can pose threats to competition whenever competitors are unable to challenge these vertical integrated firms. For example, in the case of foundation models, it has been confirmed that these are likely to become an input to other markets, like search and productivity software.[23] Hence, if a foundation model provider is vertically integrated and holds substantial market power along the AI supply chain, then it may have the incentives and capacity to develop closed ecosystems[24] that could restrain competition in other markets. Also, vertical integration could create barriers to entry if competitors need to operate at

[19] Goldfarb, A. and Trefler, D. (2019). *The Economics of Artificial Intelligence: An Agenda*, p. 469-471. *National Bureau of Economic Research*. University of Chicago Press Available at: https://www.nber.org/system/files/chapters/c14012/c14012.pdf.
[20] For example, in the United States, the average base salary for a data scientist is over USD102,000 (according to Indeed); a machine learning engineer can expect to earn a salary of USD112,421; and a software developer can expect to earn a salary of USD110,140 (according to US News). From: Reilly, J. (2023). *A cost breakdown of artificial intelligence in 2023*. Available at: https://www.akkio.com/post/a-cost-breakdown-of-artificial-intelligence-in-2022.
[21] Wang, J. (2020). *The Cost of AI Training is Improving at 50x the Speed of Moore's Law: Why It's Still Early Days for AI*. Available at: https://ark-invest.com/articles/analyst-research/ai-training/.
[22] The Economist (2023). *Is Google's 20-year dominance of search in peril?* Available at: https://www.economist.com/business/2023/02/08/is-googles-20-year-search-dominance-about-to-end.
[23] United Kingdom-CMA (2023). *AI Foundation Models: Initial review*, p. 6. Available at: https://assets.publishing.service.gov.uk/media/64528e622f62220013a6a491/AI_Foundation_Models_-_Initial_review_.pdf.
[24] United Kingdom-CMA and France-Autorité de la concurrence (2014). *The economics of open and closed systems*, pp. 20-24. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/387718/The_economics_of_open_and_closed_systems.pdf.

multiple levels of the AI stack, or a vertically integrated firm might be able to raise rivals' costs.

- **Innovation:** AI technologies development has been characterized by continuous innovation, however it has been warned that competition dynamics within a market do have an effect on innovation. According, to Aghion et. al. (2005) an increase in competition (from an initial low position) increases the rate of innovation, but with high levels of competition it is possible to observe a decrease in the rate of innovation, known as the inverted U-shaped relationship.[25] "*The reason for the inverted-U shape is that when there is not much competition, firms have little incentive to innovate. Increasing competition, accordingly, will increase the average innovation rate. But once competition is intense, increasing the competitive pressure further may result in a slower average innovation rate*."[26] In this regard, the dynamics of competition between AI providers can have an impact on the level of innovation, and even in its quality. Furthermore, it has been documented that digital providers that have been able to constitute as ecosystems and have become an important access to final consumers, have the ability and incentives to affect the rate, as well as the quality, of innovation among several markets.[27]

The aforementioned economic characteristics of AI systems could be abused to become barriers to entry and expansion of firms within the AI industry as well as in its adoption by digital providers, and they could also pose threats to competition.

3.1.1.2 Benefits from AI for consumer welfare

Consumers have benefitted from advances in technology, for example in the form of free or low-priced services, better quality goods and services, more choices, and innovative new products.[28]

Personalization can benefit consumers, as it can increase the total output and consumer welfare. For example, by lowering search costs for consumers, AI systems would be able to improve matching between the consumers' interest and the products and services they want, or getting discounts. It could also provide incentives for firms to set a lower price to consumers that would not be willing to pay the price that firms would otherwise set.[29]

However, as it will be discussed in the next sub-section, AI systems could also harm consumers and the competitive process.

3.1.1.3 Interplay between competition and consumer protection to address AI systems potential harms for consumers and competition

Some authorities have warned of the potential harms that could arise from AI systems, without adequate guidelines, policies and/or regulations to improve the transparency and

[25] Philippe, A., Bloom, N., Blundell, R., Griffith, R. and Howitt, P. (2005). "Competition and Innovation: an Inverted-U Relationship", *Quartely Journal of Economics*, No. 720, pp. 701-728. Available at: https://academic.oup.com/qje/article/120/2/701/1933966.
[26] Ezrachi, A. and Stucke, M. E. (2020). *Digitalisation and its impact on innovation*, p. 4. Available at: https://op.europa.eu/en/publication-detail/-/publication/203fa0ec-e742-11ea-ad25-01aa75ed71a1/language-en.
[27] Ezrachi, A. and Stucke, M. E. (2022). *The Tech Barons' Ideological Platter*. Available at: https://www.promarket.org/2022/08/29/the-tech-barons-ideological-platter/.
[28] United States-Department of Justice and Federal Trade Commission (2017). "Algorithms and Collusion - Note by the United States", p. 1. In *Algorithms and Collusion*. Available at: https://one.oecd.org/document/DAF/COMP/WD(2017)41/en/pdf.
[29] OECD (2019). *Challenges to Consumer Policy in the Digital Age*, p. 8. Available at: https://www.oecd.org/sti/consumer/challenges-to-consumer-policy-in-the-digital-age.pdf.

accountability from its decision-making process, limit their potential biases, and monitor the conduct of digital providers, which could pose threats to consumers.

This section presents issues regarding the interplay between consumer protection and competition policy (for a general overview of other harms that have been identified please see Annex 2).

In general, competition policy and consumer protection policy share a common goal: increase and protect consumer welfare; hence, through collaboration they can complement each other to benefit consumers. In particular, coordination and collaboration between these authorities can ensure that the application of one does not interfere with the other, this would ensure that by the implementation of certain competition policies, no unintended consequences to consumer protection arise, or vice versa. Also, coordination and collaboration can promote that these authorities share expertise and information to improve their respective duties.[30]

3.1.1.3.1 Detrimental effects on consumers' privacy and competition

It has been warned that the use of AI systems and the detailed consumer data for prediction may improve the ability of digital providers to customize products/services for consumers, potentially improving the overall surplus, but reducing consumer's surplus (more on this on section 3.3). In particular, *"companies with more data may gain a strong advantage relative to their competitors, which both enables them to extract more surplus from consumers and also relaxes price competition in the marketplace"*.[31]

In particular, Acemoglu (2021) emphasizes that:[32]

i) **Market power**: the use of AI systems and detailed consumer data for prediction may improve the ability of firms to customize products for consumers, potentially improving overall surplus, however, it also increases the power of (some) companies over consumers. The indirect effect of the better collection and processing of data by one firm is to relax price competition in the market, increasing prices and amplifying the direct distributional effects.

ii) **Behavioral manipulation**: AI systems can enable platforms to know more about consumers' preferences than they themselves do; this can lead to potential behavioral manipulation, and in such cases the platform can offer services and products that may appear as higher-quality than they truly are. Also, it has been warned that the creation of detailed profiles of individuals and using them to make predictions about individuals is also problematic because such uses may: (i) exceed the original purposes to which the individuals consented, especially when such purposes cannot be identified when the personal information was first collected; (ii) diminish the control individuals have over their own personal information; and (iii) be discriminatory or harmful towards some individuals, especially where such predictions or inferences are inaccurate.[33]

[30] OECD (2008). *The Interface between Competition and Consumer Policies*. Available at: https://www.oecd.org/regreform/sectors/40898016.pdf.
[31] Acemoglu, D. (2021). "Harms of AI", p. 4. *National Bureau of Economic Research. Working Paper 29247*. Available at: https://www.nber.org/system/files/working_papers/w29247/w29247.pdf.
[32] Acemoglu, D. (2021). "Harms of AI", pp. 13-14 and 18. In: *The Oxford Handbook of AI Governance*. (2022). Oxford University Press, 2022. Available at: https://economics.mit.edu/sites/default/files/publications/Harms%20of%20AI.pdf.
[33] Canada-Government of Canada (2021). *Privacy principles and modernized rules for a digital age*. Available at: https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/modern_1.html.

In this regard, the Furman report advised the United Kingdom's government to monitor how the use of AI systems evolves to ensure it does not lead to anti-competitive activity or consumer detriment.[34]

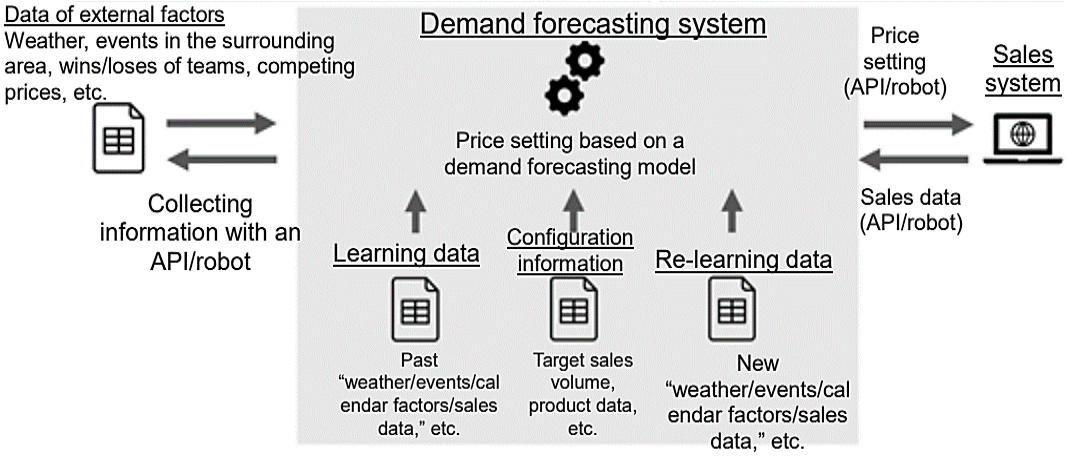
3.1.1.3.2 Effects on consumer protection and competition

Consumer protection and competition authorities have identified the following concerns in the following AI applications for consumers:[35]

i) **Personalized pricing**: advertising or setting different prices to different people (e.g. actual prices or through discounts). Personalized pricing can be understood as a type of more general dynamic pricing.[36] With the implementation of AI systems, prices could be set up according to different categories of customers and how much they are willing to pay.[37] For example, the Netherlands Authority for Consumers and Markets (ACM) found that the ecommerce website Wish was applying first-degree personalization, based on consumer's purchasing behavior and location, among other factors.[38]

The following figure presents a conceptual diagram of a price setting algorithm trained on consumers' data.

Figure 2. Example of a Price-Setting Tool Using Machine Learning



Source: Japan Fair Trade Commission (2021).[39]

From a general point of view, price personalization may lead to a net welfare loss, if the loss for consumers who pay higher prices (based on their inferred higher willingness to pay) is greater than the net gain by traders.[40] However, it is also

[34] Furman, et. al. (2019). *Unlocking digital competition: Report from the Digital Competition Expert Panel*, p. 15. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.

[35] United Kingdom-CMA (2021). *Algorithms: How they can reduce competition and harm consumers*. Available at: https://www.gov.uk/government/consultations/algorithms-competition-and-consumer-harm-call-for-information/algorithms-how-they-can-reduce-competition-and-harm-consumers.

[36] Nexocode (2023). *Dynamic Pricing Examples from the Digital Age: From Airlines to Online Retailers*. Available at: https://nexocode.com/blog/posts/examples-of-dynamic-pricing/.

[37] As firms analyze the characteristics and behavior of consumers, they could make use of ML to generate categories of consumers, and apply different treatments to each category.

[38] Netherlands- Authority for Consumers and Markets (ACM) (2022). *Following ACM actions, Wish bans fake discounts and blocks personalised pricing*. Available at: https://www.acm.nl/en/publications/following-acm-actions-wish-bans-fake-discounts-and-blocks-personalized-pricing.

[39] Japan Fair Trade Commission (2021). *Algorithms/AI and Competition Policy*, p. 16. Available at: https://www.jftc.go.jp/en/pressreleases/yearly-2021/March/210331003.pdf.

[40] IMCO (2022). *Personalised Pricing*, p. 19. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/734008/IPOL_STU(2022)734008_EN.pdf.

possible that only a fraction of consumers would be worse-off, potentially those with strong preference for certain products[41] or those which are in a lock-in situation.[42]

Furthermore, personalized pricing could harm consumers if it affects competition. In particular, it can be problematic in markets where there is insufficient competition, i.e. alternative providers cannot constraint a digital provider market power, hence this digital provider could reinforce its market power through price differentiation.[43] For example, a digital provider with market power could use personalized pricing to reduce churn (the number of customers leaving its services for another provider), or it could increase price complexity making it harder for consumers to compare prices between providers. In this case, Rhodes and Zhou (2022) prove theoretically that consumers' welfare can be worse off in a situation where only some firms can use consumer data to price discriminate while others cannot.[44]

ii) **Personalized services**:[45] digital providers present consumers with a set of options or results that are relevant to them, using extensive information about the user, for example user's location, their previous queries, and their previous browsing and purchase behavior. This information could be used to personalize a consumer journey through a website to make a purchase.

Service personalization could harm consumers when they are likely to be affected by position bias and cannot observe exactly how or why results or options are presented in a certain order. Digital providers could manipulate consumers into making decisions that are more profitable for the firm, but which the consumer would not have made under more objective or neutral conditions (see more on this on the section of dark patterns).

This could lead to 'price steering' by presenting higher priced products to consumers with a higher willingness-to-pay. Also, a digital platform may manipulate rankings of results to favor certain options, because it derives benefit from a commercial relationship, such as higher commission payments or revenue shares. In the European Union, Google was fined with EUR2.42 billion for breaching antitrust rules, for abusing its market dominance as a search engine by giving an illegal advantage to other Google products in its comparison-shopping service.[46]

3.1.1.3.3 Effects on Competition- anticompetitive practices

Consumers are affected if the competitive process is harmed. In particular, competition authorities have warned on the effects of exclusionary practices that dominant digital providers could perform to harm competitors and halt competition:

i) **Self-preferencing**: includes decisions taken by a digital provider that favors their own products or services over those of its competitors. This happens in settings where the provider is vertically integrated and participates in intermediate and final

[41] Kehoe, P. J., Larsen, B. J., and Pastorino, E. (2020). *Dynamic Competition in the Era of Big Data.* Available at: https://www.ftc.gov/system/files/documents/public_events/1567421/kehoelarsenpastorino_updated.pdf.
[42] For an example on dynamic pricing see: Uber (2017). *Engineering Extreme Event Forecasting at Uber with Recurrent Neural Networks*. Available at: https://www.uber.com/en-CA/blog/neural-networks/?utm_source=datarootlabs&utm_medium=blog.
[43] United Kingdom-Office of Fair Trading (2013). *The economics of online personalised pricing*. Available at: https://webarchive.nationalarchives.gov.uk/20140402154756/http:/oft.gov.uk/shared_oft/research/oft1488.pdf.
[44] Rhodes, A. and Zhou, J. (2022). "Personalized Pricing and Competition". Available at. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID4103763_code1584037.pdf?abstractid=4103763&mirid=1.
[45] United Kingdom-CMA (2021). Op. Cit.
[46] European Union-European Commission (2017). *Antitrust: Commission fines Google €2.42 billion* [EUR2.42 trillion] *for abusing dominance as search engine by giving illegal advantage to own comparison shopping service – Factsheet.* Available at: https://ec.europa.eu/commission/presscorner/detail/es/MEMO_17_1785.

markets. In this case, an online service provider has the ability and incentives to manipulate key algorithms and systems, e.g. ranking algorithms, to favor their own products or services where they are competing with rivals' products and services. These actions affect competitors' contestability and fairness of the competitive process, both of which harm consumers. For example, in the UK-CMA's market study of digital advertising, the authority found that vertical integration can give rise to technical efficiencies. However, integration can also raise concerns about conflicts of interest and abilities to leverage market power between adjacent markets, for example give raise to self-preferencing conducts when the digital provider operates as a provider of intermediate markets (ad tech) and final services (display of digital advertising).[47]

M. Peitz explains that dominant digital providers, by favoring first-party products and services, can distort competition between the several firms that participate in a sector and may limit the contestability or affect the competitive incentives in one or several markets. In this case, "*if a gatekeeper*[48] *reduces the visibility of superior third-party offers, third-party sellers have weaker incentives to provide such quality in the first place. Similarly, if any effort in cost reduction by a third-party seller is offset by an equivalent increase in fees charged by the gatekeeper, third-party sellers do not have an incentive to reduce their costs."*[49]

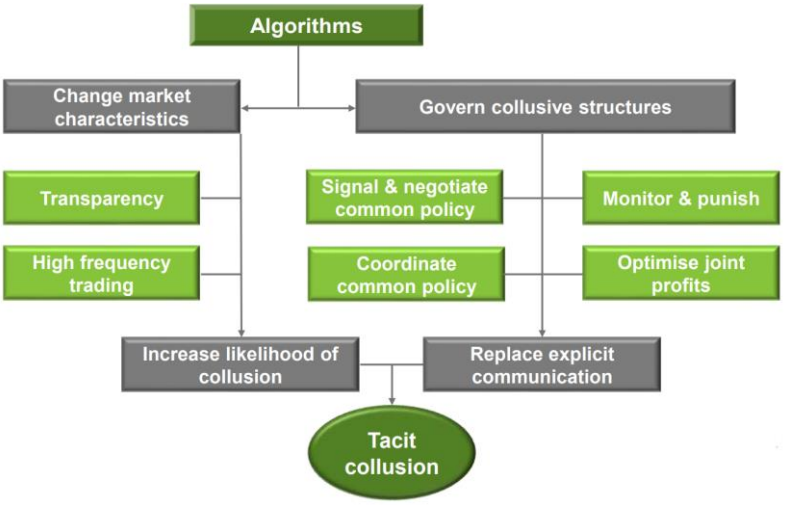
ii) **Tacit collusion by pricing algorithms**. Some authorities have stressed the possibility that AI systems could increase the chances of tacit coordination between market participants. It has been claimed that this practice could be more likely because algorithms can increase markets' transparency, speed of price changes and the calculation of optimal prices, which together create favorable market conditions for collusion.

Also, Ezrachi and Stucke (2020) explain that when firms adopt the same algorithmic pricing model, then *"the Hub-and-Spoke algorithmic structure brings us further away from typical tacit collusion"*, because while this strategy would not be indicative of a cartel agreement, it could nonetheless undermine competition.[50,51]

The following scenarios have been highlighted for increased risks of collusion: (i) the use of the same pricing algorithm by multiple market players can lead to a similar reaction to market developments and as a result similar pricing pattern; (ii) use of simple pricing algorithms which react to market conditions in a certain predictable way can increase market transparency; (iii) using the same data could increase the chances of collusion.[52]

[47] United Kingdom-CMA (2020). *Online platforms and digital advertising*, p. 176. Available at: https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf.
[48] The Digital Markets Act defines "gatekeeper" those digital platforms that provide an important gateway between business users and consumers– whose position can grant them the power to act as a private rule maker, and thus creating a bottleneck in the digital economy. European Commission (2022). *Digital Markets Act: rules for digital gatekeepers to ensure open markets enter into force.* Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6423.
[49] Peitz, M. (2022). *The Prohibition of Self-Preferencing in the DMA*. Centre on Regulation in Europe (CERRE), p. 6. Available at: https://cerre.eu/wp-content/uploads/2022/11/DMA_SelfPreferencing.pdf
[50] Ezrachi, A. and Stucke, M.E. (2020). "Sustainable and Unchallenged Algorithm Tacit Collusion", pp. 248-249. *Northwestern Journal of Technology and Intellectual Property*. Available at: https://scholarlycommons.law.northwestern.edu/njtip/vol17/iss2/2.
[51] Also see: Japan Fair Trade Commission (2021). *Algorithms/AI and Competition Policy*, pp. 19-20. Op. Cit.
[52] For further details, please see: OECD (2017). *Algorithms and Collusion: Competition Policy in the Digital Age*. Available at: www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm.

Figure 3. Risks of algorithmic collusion



Source: Gonzaga, P. (2018). *Algorithms and Collusion*.[53]

Academic literature has also warned of these potential anticompetitive conducts. For example, E. Calvano et. al. (2020) studied the behavior of AI algorithm Q-learning in a workhorse oligopoly model of repeated price competition. Calvano's results demonstrate that algorithms consistently learn to charge supra-competitive prices, without communicating with one another. The high prices are sustained by collusive strategies with a finite phase of punishment followed by a gradual return to cooperation.[54] Nonetheless, Sanchez-Cartas et. al. (2022) built a computational model that considers two sophisticated AI algorithms (Q-learning and Particle Swarm Optimization, PSO) competing in prices in three different market structures (Logit, Hotelling, and linear demand models). The results show from a consumer welfare perspective, PSO outperforms Q-learning; however, they also prove that small changes in the algorithm designs may drive both to set more competitive prices. This implies that a proper analysis of algorithmic competition requires considering the details of the algorithms and the market structure.[55]

Also, it has been warned that when firms use the same price algorithm it can lead to exchanges of competitively-sensitive information. In particular, *"[i]n some industries, high-speed, complex algorithms can ingest massive quantities of "stale," "aggregated" data from buyers and sellers to glean insights about the strategies of a competitor"*.[56] Hence, some economies are updating their guidelines to address the cases in which sharing competitively-sensitive information, through the use of same price algorithms, might constitute an infringement of competition law. For example, the European Commission revised its Horizontal Guidelines to explain in which cases the exchange of commercially sensitive information indirectly (via a third party, e.g. a firm that provides a pricing algorithm to several firms) may be constitute an infringement of competition law.[57]

[53] Available at: https://competitioncooperation.eu/wp-content/uploads/2019/01/Day-2-Session-I-Pedro-GONZAGA.pdf.
[54] Calvano, E., Calzolari, G., Denicolò, V., and Pastorello, S. (2020). "Artificial Intelligence, Algorithmic Pricing, and Collusion". *American Economic Review*, Vol. 110, No. 10. Available at: https://www.aeaweb.org/articles?id=10.1257/aer.20190623.
[55] Sanchez-Cartas, J.M. and Katsamakas, E. (2022). "Artificial Intelligence, Algorithmic Competition and Market Structures," In *IEEE Access*, vol. 10, pp. 10575-10584. Available at: https://ieeexplore.ieee.org/document/9684893.
[56] United States of America- Department of Justice, Antitrust Division (2023). *Antitrust Division Delivers Remarks at GCR Live: Law Leaders Global 2023*. Remarks made by Principal Deputy Assistant Attorney General Doha Mekki. Available at: https://www.justice.gov/opa/speech/principal-deputy-assistant-attorney-general-doha-mekki-antitrust-division-delivers-0.
[57] European Union-European Commission (2023). *Revised Horizontal Guidelines*, paragraphs 401-404. Available at: https://competition-policy.ec.europa.eu/document/fd641c1e-7415-4e60-ac21-7ab3e72045d2_en.

There have been few enforcement cases against firms that used pricing algorithms to implement explicit collusive agreements. In the United States, the DOJ charged two executives and an ecommerce retailer in a price-fixing conspiracy in which the conspirators utilized pricing algorithms to fix the prices of posters sold on the Amazon Marketplace. This case was also analyzed by the United Kingdom Competition and Markets Authority (CMA) in 2016 with a similar decision.[58]

3.1.1.3.4 Effects on Competition-Mergers and Acquisitions

In the first quarter of 2023, the M&A activity reveals that AI accounted for 186 technology deals announced, worth a total value of USD12.7 billion. The USD10 billion investment in OpenAI by Microsoft was the industry's largest disclosed deal. During the second quarter, Google's announced that it was merging its two advanced AI research labs, Google Brain and DeepMind.

According to the Furman report, the large incumbent digital providers are in the best position to lead in the next waves of technologies, with many of them likely to be based on AI systems powered by the large data sets that the incumbents have greatest access to. In this regard, it has been advised for competition authorities to update its merger policy to ensure that it can be more forward-looking and take better account of technological developments. In particular, closely consider harm to innovation and impacts on potential competition in its case selection and in its assessment of such cases.[59]

Some of the theories of harm that have been discussed are:

i) **Horizontal Theories of Harm**: loss of actual competition and potential competition. While traditionally, competition authorities have focused on the loss of actual competition, some authors are claiming that there is a need to carefully consider the impact on potential competition. This means that authorities *"would have to assess whether a smaller or nascent merging party, absent the merger, would have likely developed its service offering in a market where it is currently not active (or only active in a very limited way) so that it could compete against the acquirer"*.[60] Related to the previous, is the killer acquisition theory of harm. Bourreau and de Streel (2020) argue that in digital markets, incumbents may have more incentives to develop the innovation than the entrant which created it, including because the incumbent's significant existing user base, combined with network effects, economies of scope and potential demand-side synergies, could lead to broader scale adoption of the innovation.[61] Also, there is the reverse killer acquisition theory of harm, that involves an incumbent firm which instead of developing its own technologies, when entering in a new market, decides to acquire a target company that has already developed that functionality/capability.[62]

ii) **Vertical theories of harm**: Foreclosure through access degradation and leveraging theories of harm. Regarding the first one, in digital markets, the products offered by the merging parties may interact with each other as parts of a broader system, where

[58] United States-Department of Justice (2015). *U.S. v. David Topkins*. Available at: https://www.justice.gov/atr/case/us-v-david-topkins. See also United Kingdom-Competition and Markets Authority (2016). *Case 50223, Decision dated 12 August 2016*. Available at: https://assets.publishing.service.gov.uk/media/57ee7c2740f0b606dc000018/case-50223-final-non-confidential-infringement-decision.pdf.
[59] Furman, et. al. (2019). Op. Cit. p. 12.
[60] OECD (2023). *Theories of harm for digital mergers – Background Note*, p. 14. Available at: https://www.oecd.org/daf/competition/theories-of-harm-for-digital-mergers-2023.pdf.
[61] Bourreau, M. and de Streel, A. (2020). *Big Tech Acquisitions*. Available at: https://cerre.eu/wp-content/uploads/2020/03/cerre_big_tech_acquisitions_2020.pdf.
[62] Caffarra, C, Crawford, G. and Valletti, T. (2020). "How tech rolls': Potential competition and 'reverse' killer acquisitions", *VoxEU.org*. Available at: https://cepr.org/voxeu/blogs-and-reviews/how-tech-rolls-potential-competition-and-reverse-killer-acquisitions.

the different components need to be able to integrate and work together and interoperability is thus of paramount importance for the functioning of the system. In these cases, access degradation can take place through the degradation of interoperability. The latter regards to mergers where the merging parties are active in related markets, the merger could allow the merged entity to leverage its dominant position in one market to disadvantage or foreclose competitors in another more competitive market. For example, digital providers can achieve technical tying by integrating a product or service into another product, or through pre-installation practices.[63]

Other theories of harms[64] in digital markets, that have recently gained attention by some competition authorities, are the ecosystem-based theories of harm. In which the acquirer constitutes a digital ecosystem and by acquiring a firm that produces a product or service that is either a complement, weak substitute or unrelated product/service (related/adjacent markets) it intends to entrench and strength the dominance of the whole digital ecosystem. For example, through the merger it would be possible for the acquirer to leverage its dominance into adjacent markets. Also, related to the previous, some APEC economies have recently stressed the importance to analyze the competitive harms from serial acquisitions,[65] this means *"the addition, through acquisition, of each complementary service to the platform's ecosystem may not in itself have a material impact on competition, considered cumulatively, the acquisitions may further strengthen of the 'moat' around the platform's core service offering, thus locking-in users and entrenching the platform's dominant market position"*.[66]

Consequently, competition authorities are advised to carefully analyze the following: (i) mergers that combine two firms' datasets or AI capacity could result in market power that can be hard to contest given the substantial economies of scale and scope associated with data and AI systems; (ii) vertical mergers if the post-merger firm can cut its competitors off from the supply of an essential input (such as data or AI technology); (iii) merging parties used a different pricing strategy or algorithm from other firms in a market –meaning the merger could be depriving the market of a "maverick" that encourages competition; (iv) new theories of harms that could be especially important for digital markets, among others.[67]

3.1.1.4 Best practices on collaborative work between authorities

In the APEC region and other economies, different strategies are emerging to tackle the aforementioned potential risks and harms. In this section, some of the most relevant examples are presented.[68]

---

[63] OECD (2023). *Theories of harm for digital mergers – Background Note*, pp. 17-21. Available at: https://one.oecd.org/document/DAF/COMP(2023)6/en/pdf.

[64] For a full list of other theories of harm that might arise in digital markets, please refer to the following: OECD (2023). *Theories of harm for digital mergers – Background Note*. Available at: https://www.oecd.org/daf/competition/theories-of-harm-for-digital-mergers-2023.pdf; and OECD (2020). *Conglomerate Effects of Mergers - Background Note.* Available at: https://one.oecd.org/document/DAF/COMP(2020)2/en/pdf.

[65] Defined as strategy of a firm that, through a sequential set of acquisitions, over time, of small companies (mergers that may fall below notification thresholds) participating in the same or adjacent markets, consolidates into a larger, potentially dominant, firm (e.g. digital ecosystem).

[66] OECD (2023). *Serial Acquisitions and Industry roll-ups – Background Note*, p. 18. Available at: https://www.oecd.org/daf/competition/serial-acquisitions-and-industry-roll-ups-2023.pdf.

[67] OECD (2022). *OECD Business and Finance Outlook 2021*: *AI in Business and Finance*. Chapter 4. Competition and AI. Available at: https://www.oecd-ilibrary.org/sites/3acbe1cd-en/index.html?itemId=/content/component/3acbe1cd-en.

[68] Besides the cases presented in this section, in April 2021 the European Commission tabled a proposal for a regulatory framework on AI, Parliament voted on its position in June 2023, and EU lawmakers have started negotiations to finalize the new legislation, it is expected that it will be adopted in 2024. For further information please refer to: European Union- European Parliament (2023). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL*

The United States

In October 2023, the White House issued the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.[69] The Executive Order states that responsible AI use has the potential to help solve urgent challenges while making the world more prosperous, productive, innovative, and secure. But also warns that irresponsible use could exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and pose risks to domestic security. Consequently, it sets guiding principles and priorities to advance and govern the development and use of AI.

Also, in October 2022, the White House Office of Science and Technology Policy, issued *The Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*,[70] a whitepaper intended to *"support the development of policies and practices that protect civil rights and promote democratic values in the building, deployment, and governance of automated systems."*[71] This does not constitute a regulation, but a guidance on specific topics that the Office found problematic in the exercise of rights of the American people and AI systems.

Along with the whitepaper, the United States government is working on different fields, from the private sector[72] and specific tasks for agencies.[73] In particular, for protecting consumers:

- The Federal Trade Commission (FTC) is exploring rules to curb commercial surveillance, algorithmic discrimination, and lax data security practices that could violate section 5 of the FTC Act. The FTC has also issued guidance[74] to market participants regarding potential violations of the FTC Act that may arise by using automated tools that have discriminatory impacts, making claims about AI that are not substantiated, or to deploying AI before taking steps to assess and mitigate risks.[75] Finally, the FTC has required firms to destroy algorithms or other work products that were trained on data that should not have been collected. Some FTC's enforcement actions:
    - FTC vs Amazon (Alexa):[76] According to the complaint, Amazon repeatedly assured parents that they could request deletion of voice recordings of their children. However, Amazon did not keep its promises when it unlawfully

INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206&gid=1701706014824; and European Union- European Parliament (2023). *Artificial intelligence act. Briefing. EU Legislation in Progress*. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf.

[69] United States-White House Office (2023). *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

[70] United States-White House Office of Science and Technology Policy (2022). *The Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*. Available at: https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.

[71] Ibidem., p. 2.

[72] To foster risk management in AI among private organizations, in January 2023 the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) released its *Artificial Intelligence Risk Management Framework* (AI RMF 1.0), a guidance document for voluntary use by organizations designing, developing, deploying or using AI systems to help manage the many risks of AI technologies. In addition, NIST plans to launch a Trustworthy and Responsible AI Resource Center to help organizations put the AI RMF 1.0 into practice.

[73] Actions implemented by the time are presented in the following link: FACT SHEET: Biden-Harris Administration Announces Key Actions to Advance Tech Accountability and Protect the Rights of the American Public. Available at: https://www.whitehouse.gov/ostp/news-updates/2022/10/04/fact-sheet-biden-harris-administration-announces-key-actions-to-advance-tech-accountability-and-protect-the-rights-of-the-american-public/.

[74] United States-FTC (2023). *Keep your AI claims in check*. Available at: https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check.

[75] United States-FTC (2023). *Chatbots, deepfakes, and voice clones: AI deception for sale*. Available at: https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale.

[76] United States (2023). United States of America, Plaintiff v. AMAZON.COM, INC., a corporation, and AMAZON.COM SERVICES LLC, a limited liability company, Defendants. Available at: https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3128-amazoncom-alexa-us-v.

retained data after parents requested deletion, instead used data to improve its Alexa voice recognition algorithm. In the proposed federal court order, Amazon must delete inactive child accounts and certain voice recordings and geolocation information, and will also be prohibited from using such data to train its algorithms.

- FTC vs Ring:[77] Ring, a home security camera company, failed to adequately notify customers or obtain consent for extensive review of private video recordings for various purposes, including training algorithms. Under proposed order, Ring will be required to delete data products such as data, models, and algorithms derived from videos it unlawfully reviewed.

- To protect consumers in the financial system, the Consumer Financial Protection Bureau (CFPB) confirmed that federal anti-discrimination law requires that creditors provide consumers with specific and accurate explanations when credit applications are denied or other adverse actions are taken, even if the creditor is relying on a black-box credit model using complex algorithms.[78] CFPB is also cracking down on algorithmic discrimination in the financial sector[79] and hiring technologists to fully staff this oversight work.

Also, collaboration has spurred among different agencies. In April 2023, the Justice Department (DOJ), Equal Employment Opportunity Commission (EEOC), CFPB and FTC, issued a joint statement about enforcement efforts combatting bias from the use of automated systems and AI.[80]

Canada

In June 2022, the Government of Canada proposed the Artificial Intelligence and Data Act (AIDA) as part of Bill C-27,[81] the Digital Charter Implementation Act, 2022. The AIDA is expected to fill the regulatory gaps for AI systems, the framework intended to ensure the proactive identification and mitigation of risks in order to prevent harms and discriminatory outcomes, while recognizing the unique nature of AI ecosystem and ensuring that research and responsible innovation are supported. In this regard, the AIDA proposes the following approach:

1. **Consumer protection.** This regulation will define which systems would be considered as “High-Impact”, as well as the specific requirements. AIDA would ensure that “High-Impact AI systems” meet the same expectations with respect to safety and human rights to which Canadians are accustomed. Regulations defining which systems would be considered high-impact, as well as specific requirements, would be developed in consultation with a broad range of stakeholders to ensure that they are effective at protecting the interests of the Canadian public, while avoiding imposing an undue burden on the Canadian AI ecosystem. The Government has also proposed the Consumer Privacy Protection Act as part of Bill

[77] United States (2023). Ring, LLC. Available at: https://www.ftc.gov/legal-library/browse/cases-proceedings/2023113-ring-llc.
[78] United States- Consumer Financial Protection Bureau (2022). *CFPB Acts to Protect the Public from Black-Box Credit Models Using Complex Algorithms*. Available at: https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/.
[79] United States- Consumer Financial Protection Bureau (2022). *Cracking down on discrimination in the financial sector*. By Eric Halperin and Lorelei Salas. Available at: https://www.consumerfinance.gov/about-us/blog/cracking-down-on-discrimination-in-the-financial-sector/.
[80] United States-DoJ, EEOC, CFPB and FTC (2023). *Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems*. Available at: https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf.
[81] Canada- Parliament of Canada (2023). Bill C-27. An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts. Available at: https://www.ourcommons.ca/Committees/en/INDU/StudyActivity?studyActivityId=12157763.

C-27 to modernize this law in the context of the digital economy, and it is also undertaking broader efforts to ensure that laws governing marketplace activities and communications services keep pace. In addition, a number of other frameworks for consumer protection, human rights, and criminal law apply to the use of AI, including: The Canada Consumer Product Safety Act; The Food and Drugs Act; The Motor Vehicle Safety Act; The Bank Act; The Canadian Human Rights Act and provincial human rights laws; and the Criminal Code. Furthermore, existing consumer protection regulators are already moving to address some of the impacts of AI within their legislative authorities.

2. **New statutory duties for the Minister of Innovation, Science, and Industry**. This Ministry would be empowered to administer and enforce the AIDA, **to ensure that policy and enforcement move together as the technology evolves**. In cases where a system could result in harm or biased output, or where a contravention may have occurred, they may take actions such as: order the production of records to demonstrate compliance; or order an independent audit; and in cases where there is a risk of imminent harm, the Minister may take actions such as: order cessation of use of a system; or disclose publicly information regarding contraventions of the Act or for the purpose of preventing harm.
3. **New AI and Data Commissioner**. An office headed by a new AI and Data Commissioner, the Commissioner will be a senior official within the Ministry designated by the Minister, would be created to support of both regulatory development and the administration of the Act. The role would undergo gradual evolution of the functions of the commissioner from solely education and assistance to also include compliance and enforcement, once the Act has come into force and ecosystem adjusted. In addition to administration and enforcement of the Act, the Commissioner's work would include supporting and coordinating with other regulators to ensure consistent regulatory capacity across different contexts, as well as tracking and studying of potential systemic effects of AI systems in order to inform administrative and policy decisions.
4. **New criminal law provisions.** AIDA creates three new criminal offences to directly prohibit and address specific behaviors of concern. First, knowingly possessing or using unlawfully obtained personal information to design, develop, use or make available for use an AI system. Second, making an AI system available for use, knowing, or being reckless as to whether, it is likely to cause serious harm or substantial damage to property. Third, making an AI system available for use with intent to defraud the public and to cause substantial economic loss to an individual.

The AIDA is a regulatory framework intended to minimize the risks from High-impact AI systems, and also considers inter-operability with international frameworks such as the EU AI Act and others, and to avoid imposing undue impacts on the AI ecosystem.[82]

United Kingdom

In July 2020, the United Kingdom Competition and Markets Authority (CMA), the Information Commissioner's Office (ICO) and the Office of Communications (OFCOM) formed the

[82] The AIDA would require that appropriate measures be put in place to identify, assess, and mitigate risks of harm or biased output prior to a high-impact system being made available for use. In particular, the following are considered in the draft: (i) Human Oversight & Monitoring; (ii) Transparency; (iii) Fairness and Equity; (iv) Safety; (v) Accountability; and (vi) Validity and Robustness.

Digital Regulation Cooperation Forum (DRCF),[83] and in April 2021 the Financial Conduct Authority (FCA) joined it.

The DRCF was established to fulfill three goals: (i) **promote greater coherence**, so that where regulatory regimes intersect the DRCF helps to resolve potential tensions, offering clarity for people and industry; (ii) **work collaboratively on areas of common interest** and jointly address complex problems; and (iii) **work together to build the necessary capabilities**.

In particular, DRCF has worked on two papers regarding AI, *"The benefits and harms of algorithms: a shared perspective from the four digital regulators"* and "*Auditing algorithms: the existing landscape, role of regulators and future outlook 2022"*.

In the first, the DRCF stressed the importance of a coordinated regulatory approach to algorithmic processing. According to the authorities, collaboration between authorities is particularly important for addressing issues that cut across their regulatory remits. DRCF analyzed a range of algorithmic harms and benefits according to several shared areas of focus that were of mutual interest: (i) transparency of algorithmic processing for individuals affected by algorithmic processing; (ii) fairness, access to information, products, services and rights; resilience of infrastructure and algorithmic systems; (iii) individual autonomy for informed decision-making; and (iv) healthy competition to foster innovation and better outcomes for consumers.

The document identified key areas of cooperative intervention:

- **Regulatory sandboxes**: regulatory sandbox allows firms to test products and services in a controlled environment, and to reduce the time-to-market at potentially lower cost. It was proposed to explore ways of running sandboxes where two or more DRCF members can (subject to their particular powers) offer advice and the ability to test products and services that use algorithmic processing in a controlled environment.
- **Enforcement action**: It was proposed to explore ways to collaborate in investigations where algorithmic processing is causing harms that span the mandate of more than one regulator. There may also be opportunities for valuable joint work on supporting individuals and consumers in seeking redress over harms they believe they have incurred.
- **Establish greater consistency**: The authorities will seek more consistency about the language and terminology that is used when engaging with citizens about algorithms to enable them to better understand what algorithms are, where they're used, and the choices available to consumers.
- **Engagement with other regulators and stakeholders**: the DRCF will seek engagement with the Equality and Human Rights Commission when work on algorithmic processing and fairness is conducted, as well as with technology

[83] For further information check:
- DRFC (2020). *Embedding coherence and cooperation in the fabric of digital regulators*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/982898/DRCF_response_to_DCMS__PDF.pdf; and
- DRFC (2022). *DRCF Terms of Reference (ToR).* Available at: https://www.gov.uk/government/publications/drcf-terms-of-reference/terms-of-reference.
- DRFC (2022). *Auditing algorithms: the existing landscape, role of regulators and future outlook 2022*. Available at: https://www.gov.uk/find-digital-market-research/auditing-algorithms-the-existing-landscape-role-of-regulators-and-future-outlook-2022-drcf.

providers and professional users (e.g. media organizations, retail firms, and public services) to better understand how algorithmic processing takes place and how to achieve the benefits while minimizing harms.

Besides the efforts of DRCF, each of the regulators has engaged in specific activities related to their mandatory duties. The ICO issued a document on explaining decisions made by AI,[84] OFCOM's work on the use of AI in online content moderation.[85] Furthermore, CMA has launched a review on AI that will address the following: (i) competition and barriers to entry; (ii) impact that may have on competition in other markets; (iii) consumer protection issues.[86]

3.1.2 Digital dark patterns

"Dark patterns" is an umbrella term that refers to digital choice architectures found in online interfaces that are intended to trick or manipulate users into making choices they would not otherwise have made.[87] In particular, these digital architectures take advantage of consumers' cognitive and behavioral biases, and heuristics,[88] to steer consumers' conduct or delay access to information needed to make fully informed decisions.[89]

Academic research on dark patterns has found that its use is widespread across digital interfaces. For example, Mathur et al. (2019) used automated techniques to identify dark patterns in a survey of 53,000 product pages, from 11,000 shopping websites, and discovered 1,818 dark pattern instances.[90] Also, Gunawan et. al. (2021), affirmed that dark patterns were more common in mobile apps, by examining 240 of the most popular Android apps in the United States, it was found that 95% contained dark patterns.[91] Also in Japan, a study analyzed 200 popular mobile apps and found that most apps had dark patterns, with an average of 3.9 per app.[92] Also, it is expected that Dark Patterns will be used in technologies, such as augmented reality (AR) and virtual reality (VR).[93]

In recent years, dark patterns have gained attention by consumer protection, privacy and competition authorities, due to their effects on consumer's behavior, autonomy, privacy and psychology, as well as their implications on competition. However, there is still no consensus on the definition of dark patterns, mainly because dark patterns may take various forms, which implies limitations for public policy enforcement. Furthermore, as dark pattern terminology differs across jurisdictions, this could make it difficult to adopt cross-border measures.

---

[84] United Kingdom- Information Commissioner's Office and The Alan Turing Institute (2020). *Explaining decisions made with AI*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/.

[85] United Kingdom-OFCOM (2019). *Use of AI in online content moderation*. Available at: https://www.ofcom.org.uk/research-and-data/internet-and-on-demand-research/online-content-moderation.

[86] United Kingdom-CMA (2023). *AI Foundation Models: Initial review*, p. 6. Available at: https://assets.publishing.service.gov.uk/media/64528e622f62220013a6a491/AI_Foundation_Models_-_Initial_review_.pdf.

[87] Some general definitions can be found in the following: Brignull, H (2010). *Dark patterns*. Available at: https://darkpatterns.org/; and Stanford Digital Civil Society Lab (2023). *Dark Patterns Tip Line*. Available at: https://darkpatternstipline.org/.

[88] OECD (2022). *Digital Commercial Patterns*, p. 8. Available at: https://www.oecd-ilibrary.org/science-and-technology/dark-commercial-patterns_44f5e846-en.

[89] FTC (2021). *Bringing Dark Patterns to Light: An FTC Workshop. Transcript*, p. 15. Available at: https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf; and FTC (2022). *Bringing Dark Patterns to Light. Staff Report*, p.2. Available at: https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

[90] Mathur, A., Acar, G., Friedman, M.J., Lucherini, E., Mayer, J., Chetty, M., and Narayanan, A. (2019). "Dark patterns at scale: Findings from a crawl of 11K shopping websites". *Proceedings of the ACM on Human-Computer Interaction*, Vol. CSCW/81. Available at: https://doi.org/10.1145/3359183.

[91] Gunawan, J., Pradeep, A., Chofnes, D., Hartzog, W. and Wilson, C. (2021). "A Comparative Study of Dark Patterns Across Mobile and Web Modalities." *Proceedings of the ACM on Human-Computer Interaction*, Vol. CSCW2/377. Available at: https://doi.org/10.1145/3479521.

[92] Hidaka, S., Kobuki, S., Watanabe, M. and Seaborn, K. (2023). "Linguistic Dead-Ends and Alphabet Soup: Finding Dark Patterns in Japanese Apps." In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, April 23-28, 2023, Hamburg, Germany. Available at: https://doi.org/10.1145/3544548.3580942.

[93] Wang, X., Lee, L.-H., Fernandez, C. B., & Hui, P. (2023). "The Dark Side of Augmented Reality: Exploring Manipulative Designs in AR." In *International Journal of Human Computer Interaction*, pp. 1–16. Available at: https://arxiv.org/abs/2303.02843.

For the purposes of this document dark patterns will be defined as practices that modify intentionally the digital choice architecture presented to the consumer, either by modifying the set of choices available or by manipulating the information flow to the consumer,[94] with the aim to subvert or impair user autonomy, decision-making, or choice.[95] However, the appropriate definition may depend, among others, on its intended application (policy analysis or regulatory), on the legal context, and on technological and regulatory developments. (For an example of a taxonomy on dark patterns and examples, please see Annex 3.)

Regarding their effects, it has been found that dark patterns can:[96]

- **Distort consumers behavior and cause them harm by**: making consumers buy more than they want or need and at higher prices, or even harms related to autonomy, privacy and cognitive burdens.
- **Weaken or distort competition by**: incentivizing businesses to compete on attributes and invest into innovation that does not benefit consumers; and
- **Help digital providers to maintain, leverage and exploit market power by**: making it easier to retain customers or redirect them within digital ecosystems.

Considering the above, in the following subsections it will address how the use of dark patterns can distort consumer decision making, weaken competition, and enable businesses to strengthen or exploit market power.[97]

3.1.2.1 Risks to consumers and competition

3.1.2.1.1 Detrimental effects on consumers

In this section it will be presented academic research and studies from authorities and international organizations regarding the effects of dark patterns on consumer decision-making and competition.[98]

Dark patterns compromise consumers' autonomy whenever they lead consumers to make choices they may not otherwise have made, deny choice, obscure available choices, or burden the exercise of choice. In particular, those that force action or obstruct it; those which aim to interfere with it or sneaking it. Consequently, regardless of market power, dark patterns have the potential to distort consumer behavior and decision making.[99]

[94] Mathur, A., Kshirsagar. M. and Mayer, J. (2021). "What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods", In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Available at: https://arxiv.org/abs/2101.04843.

[95] European Parliament (2022). *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)*, parag. 70. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC.

[96] United Kingdom-CMA (2022). *Discussion Paper, Online Choice Architecture: How digital design can harm competition and consumers*. April 2022. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf.

[97] United Kingdom-CMA (2022). *Discussion Paper, Online Choice Architecture: How digital design can harm competition and consumers*. April 2022. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf

[98] OECD (2020). "Chapter 8. Consumer policy in the digital transformation", Using behavioural insights to address consumer policy challenges in the digital transformation. In *OECD Digital Economy Outlook 2020*. Op. Cit.

[99] United Kingdom- ICO and CMA (2022). *Harmful design in digital markets: How Online Choice Architecture practices can undermine consumer choice and control over personal information*. Available at: https://www.drcf.org.uk/__data/assets/pdf_file/0024/266226/Harmful-Design-in-Digital-Markets-ICO-CMA-joint-position-paper.pdf.

In general, consumer detriment from dark patterns can be broadly divided into three categories: (i) economic harms, (ii) privacy harms, and (iii) cognitive burdens. For the purposes of this document this section will focus on the first two.

Economic harms

Dark patterns under this category can be considered as unfair commercial practices that harm consumers' economic interests and could violate consumer protection laws. In general, economic harms can be subdivided into:[100]

1. Dark patterns may induce consumers to purchase products or services which they may have otherwise not chosen to purchase, leading to an inefficient allocation of products.
2. Dark patterns may allow sellers to charge more for products than what consumers otherwise would be willing to pay.

Some examples of dark patterns designed to directly induce higher one-off purchases are: hidden costs, drip pricing, scarcity cues or preselection, which can have an effect on; while "hard to cancel subscriptions" could harm consumers on ongoing basis.

Some evidence from academic literature and consumer enforcement can shed light on the magnitude of detriment. However, measuring harms is challenging because (i) different dark patterns may be used by a specific provider, so the accumulative effect must be considered, and (ii) results are highly dependent on the methodological set-up.

It has been found that use of "drip pricing" resulted in consumers spending 21% more than otherwise.[101] For example, in 2017 the UK-CMA's investigation into hotel booking sites, for misleading activity messages and scarcity claims, misleading discount claims, incorrect reference pricing and hidden charges, led to the subsequent alignment of such practices with UK consumer laws with benefits to consumers estimated at GBP34 million (OECD, 2021[9]).[102]

Privacy harms

Dark patterns effects on privacy have also gained substantial attention from academics and privacy authorities.

Some relevant examples of privacy-intrusive dark patterns are: (i) preselection—privacy-intrusive settings as the default—, (ii) forced disclosure, hidden information and hard to cancel, that make privacy-related choices or information hard to obtain or opt out of; and (iii) nagging, which induce the consumer into accepting privacy-intrusive settings. In all of these cases, consumers may end up providing more personal data than intended, potentially exposing them to further risks.[103]

In the academic literature, Graßl et al. (2021) demonstrated –through two experiments–that most of the participants accepted all cookies regardless of the type of dark pattern they

[100] European Union-European Commission, Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F. Liva, G., Lechardoy, L. et al. (2022). *Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation: final report*, p. 90. Publications Office of the European Union. Available at: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418.

[101] Blake, T., Moshary, S. Sweeney, K., Tadelis, S. (2021). "Price Salience and Product Choice", *Marketing Science*, Vol. 40/4, p. 43, Available at: https://pubsonline.informs.org/doi/10.1287/mksc.2020.1261.

[102] United Kingdom-CMA (2017). *Online Hotel Booking*. Available at: https://www.gov.uk/cma-cases/online-hotel-booking.

[103] OECD (2022). Op. Cit. p. 25. and Bösch, C., Erb, B., Kargl, F., Kopp, H., and Pfattheicher, S. (2016). "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns". In *Proceedings on Privacy Enhancing Technologies*, Vol. 4, pp. 237–254. Available at: https://www.petsymposium.org/2016/files/papers/Tales_from_the_Dark_Side__Privacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf.

faced, as opposed to bright patterns that encouraged the protection of their privacy.[104] Also, the Chilean Consumer Protection Authority (SERNAC) conducted a study on the impact of dark patterns on consumer decisions vis-à-vis cookie consent requests, which concluded that dark pattern (especially in cases where the choice architecture encourages the acceptance of cookies[105]) can remain highly effective even if individuals have more freedom to make privacy choices or information about practices of businesses.[106]

Assessing the magnitude of privacy harms due to dark patterns is even more challenging than the economic harms, because agencies require a quantifiable indicator, which in most cases has not been developed; and consumer complaints may be absent, since consumers may be not aware that they have taken an influenced decision or they are not aware they are paying for non-price services with their data. Despite the difficulties with defining dark patterns with precision, some privacy enforcement authorities regard certain uses of dark patterns as violating data protection and privacy laws and have already taken regulatory actions against businesses employing them.

Some academic studies have shed light on some quantitative methodologies to assess the amount of harm. For example, Morton and Dinielli (2020) conceptualized the detriment from privacy-intrusive dark patterns as a higher "data price" than they would freely choose in exchange for the quality of the service.[107] Alternatively, Gunawan, Choffnes and Wilson suggest that measuring the level of effort required to avoid a privacy-intrusive dark pattern could provide insight into the magnitude of its harm.[108]

3.1.2.1.2 Detrimental effects on competition

The use of dark patterns can undermine competition in several ways, as the United Kingdom CMA has identified it can weaken competitive process and enhance market power.

Distortions to the competitive process

In particular, it has been identified that dark patterns can weaken or distort the competitive process by shifting the incentive to compete on product attributes that benefit the consumer, such as quality and price, towards less relevant or beneficial attributes, such as salience.[109]

The generalized market use of dark patterns can distort the competitive process as a whole if dark patterns impede consumers' ability to select firms based on the merits of their product offerings.[110] Also, market efficiency could be hampered whenever dark patterns increase transaction costs for consumers, for example increasing the cost of effectively evaluating the advantages and disadvantages between options[111] or by increasing the costs of

[104] Graßl, P. Schraffenberger; H., Zuiderveen Borgesius, F., Buijzen, M. (2021). "Dark and Bright Patterns in Cookie Consent Requests", *Journal of Digital Social Research*, Vol. 3/1, pp. 1-38. Available at: https://jdsr.se/ojs/index.php/jdsr/article/view/54.
[105] In particular, when comparing experimental conditions with identical content but different aesthetic manipulations, the results show that 94.48% of the participants in the "dark pattern with more information" treatment accept all additional cookies, while 67.17% of the participants in the "bright pattern with more information" treatment choose to reject them. The results demonstrate the relevant impact that minor alterations have on users' privacy decisions.
[106] Chile-Servicio Nacional del Consumidor (2023). *Policy Paper On Cookies Consent Requests: Experimental Evidence Of Privacy By Default And Dark Patterns On Consumer Privacy Decision Making*. Available at: https://icpen.org/sites/default/files/2022-05/SERNAC_Policy_Paper_Cookies_Experiment.pdf.
[107] Scott Morton, F.M. and Dinielli, D.C. (2022). "Roadmap for an Antitrust Case Against Facebook". *Stanford Journal of Law, Business & Finance*. Available at: https://omidyar.com/wp-content/uploads/2020/09/Roadmap-for-an-Antitrust-Case-Against-Facebook.pdf.
[108] Gunawan, J., Pradeep, A., Choffnes, D. Hartzog, W. and Christo, W. (2021). "A Comparative Study of Dark Patterns Across Mobile and Web Modalities". In *Proceedings of the ACM 2021 Conference on Computer-Supported Cooperative Work and Social Computing*, Vol. 5, No. CSCW2, Article 377. Available at: https://www.ftc.gov/system/files/ftc_gov/pdf/PrivacyCon-2022-Gunawan-Pradeep-Choffnes-Hartzog-Wilson-A-Comparative-Study-of-Dark-Patterns-Across-Mobile-and-Web-Modalities.pdf.
[109] United Kingdom-CMA (2022). Op. Cit. pp. 29-32.
[110] Kemp, K. (2020). "Concealed data practices and competition law: why privacy matters", *European Competition Journal*, Vol. 16/2-3, pp. 628-672. Available at: https://doi.org/10.1080/17441056.2020.1839228.
[111] Stigler Centre (2019). *Committee for the Study of Digital Platforms. Market Structure and Antitrust Subcommittee: Report*. George J. Stigler Center for the Study of the Economy and the State. The University of Chicago Booth School of Business. Available at: https://research.chicagobooth.edu/-/media/research/stigler/pdfs/market-structure---report-as-of-15-may-2019.pdf.

implementing such choices.[112] Furthermore, some academics have highlighted the risks of a suboptimal "phishing equilibrium", when providers compete using deceptive methods.[113]

In this regard, Rasch, Thöne and Wenzel (2020) found that through drip pricing it was possible to reduce price transparency, and this hindered consumers' ability to identify the lowest price.[114] Also, the Australian-ACCC identified dark patterns that hinder switching between online browsers, and it concluded that such conducts discourage consumers from switching to alternative providers and make it difficult for consumers to exercise choice.[115]

Enhancing market dominant position of digital platforms

Dark patterns can help businesses that have market power to maintain it by limiting competition or squeezing rivals out and they could also be used to leverage a position of market power in other markets, or to exploit their customers.

In the first case, digital providers that aim to increase or maintain its high market share through customer retention may use practices like default auto-renewal followed by high levels of sludge to prevent customers from switching away.

In the second, a dominant firm could also use dark patterns to leverage its position to obtain market power in a related or downstream market.[116] In this regard, in the case of European Commission against Google Shopping, on self-preferencing demonstrated that Google used a dark pattern, in the form of algorithmic bias, against competitors.[117]

In general, the exploitation of market power may lead to higher prices and lower quality, unfair contracts, compulsory data sharing, and limited options for switching.

3.1.2.2 Best international practices

The United States

Section 5 of the Federal Trade Commission Act prohibits *"unfair or deceptive acts or practices in or affecting commerce"* and contains principle-based prohibitions on these. The FTC considers a deceptive act or practice to be any representation, omission, or practice that is both: (i) material and (ii) likely to mislead consumers who are acting reasonably under the circumstances.[118] An unfair trade practice is defined as one that:

i. causes or is likely to cause substantial injury to consumers,

ii. is not reasonably avoidable by consumers themselves, and

iii. is not outweighed by countervailing benefits to consumers or competition.

---

[112] Shahab, S. and Lades, L.K. (2021). "Sludge and transaction costs", *Behavioural Public Policy*, 2021. Available at: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/D09206BF9B36C129F40A27A9E749074B/S2398063X21000129a.pdf/sludge-and-transaction-costs.pdf.

[113] Willis, L. (2020). "Deception by Design", *Harvard Journal of Law & Technology*, Vol. 34/1, pp. 115-190. Available at: https://jolt.law.harvard.edu/assets/articlePDFs/v34/3.-Willis-Images-In-Color.pdf.

[114] Rasch, A., Thöne, M., and Wenzel, T. (2020). "Drip pricing and its regulation: Experimental evidence". *Journal of Economic Behavior & Organization*, Vol. 176, August 2020, pp. 353-370. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0167268120301189.

[115] Australia-Australian Competition & Consumer Commission (ACCC) (2021). *Digital platform services inquiry*, p. 17. Available at: https://www.accc.gov.au/system/files/DPB%20-%20DPSI%20-%20September%202021%20-%20Full%20Report%20-%2030%20September%202021%20%283%29_1.pdf.

[116] Day, G. and Stemler A. (2020). "Are Dark Patterns Anticompetitive?", *Alabama Law Review*, Vol. 72/1. Available at: https://www.law.ua.edu/lawreview/files/2020/11/1-DayStemler-1-45.pdf.

[117] Himes, J. and Crevier, J. (2021). "Something Is Happening Here but You Don't Know What It Is. Do You, Mrs. Jones?" Dark Patterns as an Antitrust Violation. In *Competition Policy International website.* Available at: https://www.competitionpolicyinternational.com/something-is-happening-here-but-you-dont-know-what-it-is-do-you-mrs-jones-dark-patterns-as-an-antitrust-violation/.

[118] United States-FTC (2023). *Federal Trade Commission Act*. 15 U.S.C. §§ 41-58, as amended. Available at: https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act.

United States law also provides for express prohibitions on specific practices. In particular, in 2023, *Guides Against Bait Advertising* was amended to include express prohibitions on specific practices found in dark patterns, such as on bait and switch practices.[119] Also, the *Restore Online Shoppers' Confidence Act* forbids charging a consumer for a good or service after an initial transaction without the consumer's express informed consent and prohibits on data-pass used to facilitate certain deceptive Internet sales transactions.[120]

As part of its advocacy work, in 2021, the FTC issued an enforcement policy statement that warned companies against deploying illegal practices that trick or trap consumers into subscription services. For example, advertising and promotional messages integrated into and presented as non-commercial content.[121]

In 2022, the FTC issued a report on dark patterns, presenting its taxonomy, legal framework, common examples of dark patterns and made recommendations for digital interface designs to comply with privacy, consumer and competition law.[122] To gather information, FTC had conducted a workshop[123] with experts from different fields, where the panelists noted that the use of manipulative design techniques in the digital world can pose heightened risks to consumers.

In February 2023, the FTC launched the Office of Technology, to support the FTC's law enforcement and policy work in the digital marketplace. The Office of Technology will contribute to the FTC's mission by: (i) strengthening and supporting law enforcement investigations and actions; (ii) advising and engaging with FTC staff and the Commission on policy and research initiatives; and (iii) engaging with the public and relevant experts to understand trends and to advance the Commission's work.[124]

Furthermore, some states have privacy legislations that explicitly ban deceptive design patterns. For example, in the state of California, the California Privacy Protection Agency enforces the California Privacy Rights Act [125] that includes specific definitions and sanctions regarding the use of dark patterns.

European Union

The Digital Services Act (DSA) prohibits online platforms from designing, organizing or operating online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of recipients of their service to make free and informed decisions. The DSA further provides that the European Commission may issue guidance on how the prohibition applies in relation to specific dark patterns – particularly false hierarchy, nagging and hard to cancel.

In the Digital Markets Act it was established that gatekeepers shall not degrade the conditions or quality of any of the core platform services provided to business users or end users who avail themselves of the rights or choices or make the exercise of those rights or

[119] United States-FTC (2023). *16 CFR Part 238 -- Guides Against Bait Advertising*. Available at: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-B/part-238.
[120] United States (2023). Online Shoppers' Protection, 15 U.S.C. §§ 8401- 8405, Prohibitions against certain unfair and deceptive Internet sales practices. Available at: https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter110&edition=prelim.
[121] United States-FTC (2021). *Enforcement Policy Statement Regarding Negative Option Marketing*, 86 Fed. Reg 60822. Available at https://www.ftc.gov/system/files/documents/public_statements/1598063/negative_option_policy_statement-10-22- 2021-tobureau.pdf
[122] United States-FTC (2022). *Bringing Dark Patterns to Light.* Staff Report. Available at: https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.
[123] Transcript of the workshop can be accessed in the following link: https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf.
[124] United States-FTC (2023). *FTC Launches New Office of Technology to Bolster Agency's Work*. Available at: https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-launches-new-office-technology-bolster-agencys-work.
[125] United States- California- California Privacy Protection Agency (2023). *California Privacy Rights Act.* Available at: https://cppa.ca.gov/regulations/.

choices unduly difficult, including by offering choices to the end-user in a non-neutral manner, or by subverting end users' or business users' autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface or a part thereof.

As part of the continuous efforts to enforce consumer protection, in January 2023 the European Commission and National Consumer Protection authorities of 23 Member States, Norway and Iceland, released the results of a screening ("sweep") of retail websites. This check covered 399 online shops of retail traders selling products ranging from textiles to electronic goods. The results showed that that nearly 40% of the online shopping websites rely on manipulative practices to exploit consumers' vulnerabilities or trick them.[126] Given these results, domestic consumer protection authorities are contacting the traders concerned to rectify their websites and take further action if necessary, according to their domestic procedures.[127]

[126] European Union- Enforcement of consumer protection (2022). *Sweep on dark patterns*. Available at: https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/sweeps_en.
[127] European Union-European Commission- (2023). *Consumer protection: manipulative online practices found on 148 out of 399 online shops screened*-Press Release. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418.

3.2 Online safety, regulatory and competition issues

Digital transformation has fostered the creation of new and innovative online business models and online services, such as online social networks and video-sharing platforms,[128] which have allowed business users and internet users to access information and engage in transactions in novel ways. However, internet users could be exposed to risks and harms online, for example, from the spread of illegal or harmful content, that risk their fundamental rights and could also lead to societal harms.

Currently, in many economies it is largely up to individual online providers to establish rules and guidelines for the types of activity and content that are or are not permitted on their platforms, in many cases the guidelines are included in their terms of service. However, these can diverge significantly across services. For this reason, some economies around the world are introducing, or are considering introducing guidelines, domestic laws and/or regulations on online safety. In some cases, they are imposing diligence requirements as regards to the way they should tackle illegal content, online disinformation or other societal risks. In these regulations and laws, it has been warned that while online harms and risks issues could be widespread across the internet, higher risks come from very large online platforms given their reach and the multiplicity of their activities.

It is acknowledged that there are differences in how economies define online risks and harms, and that there is no international consensus on how to define or categorize online harms. Nonetheless, for the purposes of this document we will focus on digital platforms that provide content services, and online harms will be considered on the basis of human and consumer rights, emphasizing the impacts on individual internet users and society.

The section is divided as follows. First, it presents the main aspects of digital platforms' business models, how do they operate, the main economic aspects and competition dynamics. Second, it presents a brief summary on online safety and competition concerns. Third, it will be presented three case studies of jurisdictions that have introduced online safety laws.

3.2.1 Business model, economic characteristics and competition dynamics

This section will explain the business model and competition dynamics of "zero-price" online platforms (platform intermediaries). Online platforms that provide "zero-price" services are important from an economic and societal perspective, as they have the higher number of active users, so they would imply higher risks given their reach and the multiplicity of their digital activities.

3.2.1.1 Business model

Online platforms that provide "zero-price" digital services to consumers (audience) rely on a business model that is mainly funded through: (i) commissions paid by business users of platforms, and/or (ii) through digital advertising (digital spaces located within their webpages or apps).[129] In the latter, digital platforms bundle content and advertising to be seen by internet users in exchange for their attention to targeted ads and their data

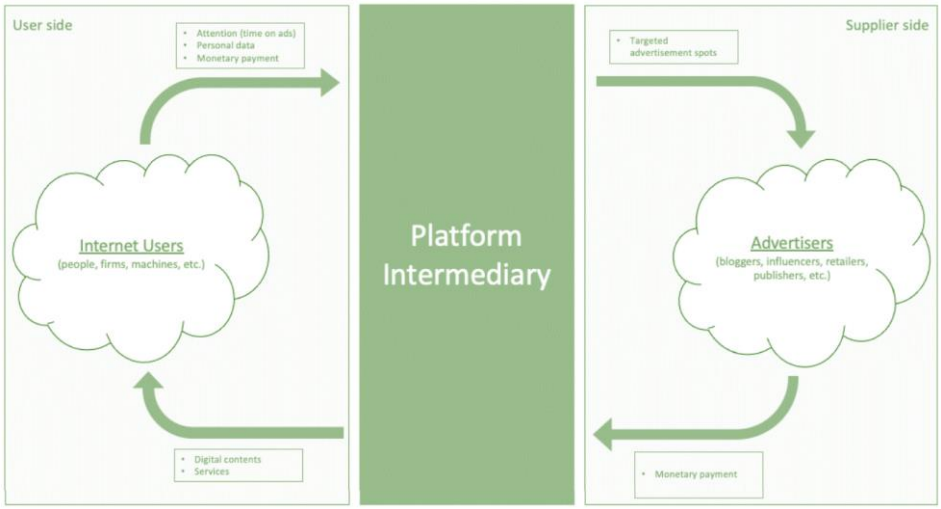
[128] "Video-sharing platforms" are a type of online video service which allow users to upload and share videos with the public. OFCOM (2022). *Video Sharing Platforms: Ofcom's Plan and Approach*. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0016/226303/vsp-plan-approach.pdf.

[129] This type of digital providers can also provide other services within the Ad tech stack or other digital services (e.g. market places).

(personal information and digital traces).[130] Some authors, have coined the term "attention brokers" for this type of platform model.[131]

This business model has been defined in economic literature as two-sided markets.[132] Digital platforms act as intermediaries between at least two different types of users of the platform, and help them to generate interactions —solve a transaction problem—, in this case, between advertisers and the audience (final consumers).[133] Furthermore, as digital platforms are able to collect and process a vast amount of information about user's behaviors, preferences, interests, geographical location, among many others, they can use this information strategically; for example, to sell advertising spaces, improve their own services, develop new businesses, etc.

Figure 4. Digital Platforms as two-sided markets



Source: Prado, Tiago S. (2021).[134]

Determining how online platforms profit from zero-price strategies[135] sheds light on whether they could raise [136] privacy and online safety concerns.

3.2.1.2 Economic characteristics

Among the most relevant economic characteristics of, for example, content platforms, are the following:[137]

i) **Two (or multisided) markets**: In two-sided markets, there are three distinctive economic characteristics: (i) the firm is multiproduct: it provides a distinct service to two sides of the market and can explicitly charge different prices; (ii) cross-

[130] M. Delrahim (2019). *""I'm Free": Platforms and Antitrust Enforcement in the Zero-Price Economy"*, p.2. Remarks as Prepared for Delivery at Silicon Flatirons, University of Colorado Law School, Department of Justice. Available at: https://www.justice.gov/opa/speech/file/1131006/download.
[131] Prat, A. and Valletti, T. (2022)."Attention Oligopoly." In *American Economic Journal: Microeconomics*, Vol. 14 (3): 530-57. Available at: https://www.aeaweb.org/articles?id=10.1257/mic.20200134.
[132] Nonetheless, J. M. Newman (2020) has contested the view of a two-sided market analysis for antitrust enforcement action.
[133] Evans, D. (2020). *The Economics of Attention Markets*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3044858.
[134] Prado, T. (2021). *Assessing the Market Power of Digital Platforms*.In: 23rd Biennial Conference of the International Telecommunications Society (ITS): "Digital societies and industrial transformations: Policies, markets, and technologies in a post-Covid world", Online Conference / Gothenburg, Sweden, 21st-23rd June, 2021. Available at: https://www.econstor.eu/bitstream/10419/238048/1/Prado-Assessing.pdf.
[135] Other types of business strategies which use zero-price strategies are: (i) tying/bundling related products, in this case the provider ties or bundles a paid service to a non-priced service, this could be an integral part of the paid-service, this strategy can be profit-maximizing if the offer of a free product increases demand for the positive-price good; (ii) premium upgrades (freemium), in this strategy the free version is expected to attract consumers to test out the product, with the hope that some consumers will upgrade to the paid version: (iii) temporary offers, platforms also may offer a new product for free during its beta-testing phase to help measure consumer demand and improve the product before its official launch. From M. Delrahim (2019), p. 6.
[136] Michal S. G. and Rubinfeld, D. L. (2016). "The Hidden Costs of Free Goods: Implications for Antitrust Enforcement", *Antitrust Law Journal*, No. 80, p. 548. Available at: https://www.law.berkeley.edu/wp-content/uploads/2015/04/80AntitrustLJ521_stamped.pdf.
[137] European Union-European Commission (2002). *Market Definition in the Media industry -Economic Issues-*, https://ec.europa.eu/competition/sectors/media/documents/european_economics.pdf.

network effects: users' participation depends on the user's participation on the other side of the market; (iii) platforms are price setters on both sides of the market. For the case of online platform intermediaries, they provide two different services to the two distinct groups they serve, and for which they charge different prices. On one side of the platform, consumers engage with the platform to watch content; on the other, advertisers pay the digital platform to present ads to the audience (e.g. sponsored content, video ads, ban ads, etc.). Regarding cross-network effects, studies have demonstrated that consumers (audience), on average, report dis-utilities from advertising, while advertisers derive a positive indirect network effect, the higher the audience the more they are willing to pay to present ads in the digital platform.[138] Some academic authors have coined the term "attention platforms" to refer to this type of digital providers (i.e. attention brokers). The importance of attention as a product to be exchangeable has important implications for business models and competition between digital providers.

ii) **Attention is scarce**: Wu (2019) explains that users' attention is scarce, since: (i) the brain has a limited capacity to process information; (ii) we are limited by time; and (iii) humans make "attentional decisions", consumers decide to pay attention to some things, according to their preferences. Consequently, digital platforms make decisions on the "attentional price" which means they decide how much content and advertising they bundle together.[139] When digital platforms decide on how much advertising they present, they are deciding on the quality of their service. Since, there is a fixed physical or temporal capacity constraint for each bundle, an increase in the amount of space devoted to ads results in an exact opposite decrease in the amount of space devoted to content.

iii) **Economies of scale:** The cost structure of producing content frequently involves substantial economies of scale. In general, content can be described as non-rivalrous good because, once created, the information good itself (rather than its distribution) can always be provided to an additional consumer at zero marginal cost of production. Consequently, economies of scale in content production are an inherent feature of these markets, as more consumers experience content, the average cost of the content production decreases.

Furthermore, the cost of producing some type of content has decreased due to technological innovations. For example, users of video sharing platforms, such as YouTube, Facebook and Instagram, can produce their own content using their mobile phones or with cameras installed in their laptops/desktops. However, the cost of producing or acquiring licencing rights of certain content –mainly premium content, high budget movies and series, or premiere live sport or music events–, still remains high. The latter case exemplifies the type of content for which digital platforms may charge audience for watching it (e.g. pay-per-view), and rely on other type of business models.

[138] A general theoretical framework regarding pricing strategies in multi-sided platforms have been explained by Weyl, E. G. (2010). "A Price Theory of Multi-Sided Platforms." *The American Economic Review*, No. 100 (4), pp. 1642–1672. Available at: http://www.jstor.org/stable/27871269.

[139] Wu, T. (2019). Blind Spot: The Attention Economy and the Law. *Antitrust Law Journal*, Vol. 82. Available at: https://scholarship.law.columbia.edu/faculty_scholarship/2029/

iv) **Economies of scope:** Economies of scope occur when producing a wider variety of goods or services in tandem is more cost effective for a firm than producing less of a variety or producing each good independently. In content production, it is always more cost effective to produce different kind of content, such as movies, series, tv programs (sports, news, magazine, etc.), that can be distributed by the same means, and uses similar inputs (talent, studios, etc.).

v) **Economies of scale and scope from data:** digital platforms, such as social media platforms or OTT content services, use data for two main purposes: (i) **improve their services**, for example, they can use algorithms to present content that is more relevant to users, also these recommendation systems become more accurate as more data is provided,[140] and (ii) **targeted advertising**, data analysis allows these services to characterize and target consumers to show them relevant advertisement.[141]

   The more detailed the data, the wider the range of transactions, the bigger the user sample, the greater the company's analytics experience (Barwise and Watkins, 2018[142]). Data is an important asset for digital services, a great number of them found their business model on analysis made on data they extract from their users, hence they either sell their datasets to data brokers or can offer targeted advertising.

vi) **Direct network effects:** certain digital platforms may exhibit strong network effects on the user's side. This means that as more users are on that side there would be more users interested in using it. Strong direct network effects can increase the barriers to entry and to expansion and prevent the development of effective competition. In markets where direct network effects play an important role, early entrants can enjoy first-mover advantage and command a dominant position in a market that is durable and difficult for later entrants to disrupt. This can result in highly concentrated markets and dominant companies with market power. Hence, by increasing barriers to entry, network effects can be an important factor in competition dynamics.

vii) **Single-homing and multi-homing**: The situation when a group of consumers uses only one platform provider to access a certain service is known as single-homing. Multi-homing refers to a group of consumers that uses more than one alternative service. The decision whether to multi-home or not depends on different elements, ranging from the existence of significant switching costs to consumer's preferences. For example, CMA's (2020[143]) market study on Digital Advertising analyzed the lack of multi-homing on the side of users for social media, and explained that these were due to factors such as limited interoperability as well as the time cost for consumers to set up an account on another platform.

[140] Fayyaz, Z., Ebrahimian, M., Nawara, D., Ibrahim, A., Kashef, R. (2020). "Recommendation Systems: Algorithms, Challenges, Metrics, and Business Opportunities." *Applied Sciences*. Vol 10 (21). Available at: https://doi.org/10.3390/app10217748.
[141] APEC (2019). *Project Report on Competition Policy for Regulating Online Platforms in the APEC Region*. Available at: https://www.apec.org/publications/2019/08/competition-policy-for-regulating-online-platforms-in-the-apec-region.
[142] Barwise, P. and Watkins, L. (2018). "The evolution of digital dominance", In *Digital Dominance: The power of Google, Amazon, Facebook, and Apple*, Editors M. Moore and D. Tambini, Oxford University Press. Available at: https://lbsresearch.london.edu/id/eprint/914/1/9780190845124_Barwise_Chapter%201.pdf.
[143] United Kingdom-CMA (2020). *Online platforms and digital advertising. Market study final report*. Available at: https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf.

viii) **Vertical Integration and ecosystems**: Some digital platforms have established extensive ecosystems of related or complementary products and services. Platform ecosystems benefit consumers by making it easier to move between services and devices within the same ecosystem. However, limited interoperability between different online platform ecosystems, in combination with default biases, can result in limited competition in services supplied within platform ecosystems, and potentially limited competition between ecosystems themselves.[144] Furthermore, growing vertical integration and ecosystems have the potential to affect competition where they extend the dominance of a platform in one market into adjacent markets, such as when a platform's complementary products and services could insulate their core service from future competition, and where it provides platforms with additional opportunities to gather data.

For the reasons outlined above, many digital markets can result in a small number of platforms holding a high share of participation that persists over time. This situation can lead to concentrated market structures with one or only a few providers, and with very asymmetric participation rates. Markets with these combined features are prone to tipping —a cycle leading to a dominant firm and high concentration.

3.2.1.3 Competition dynamics

As explained earlier, these digital platforms offer the audience (final consumers) bundles of content and ads, so they compete for audience and advertisement. In this subsection, it will be explained how digital platforms compete to increase users' reach and attention, in terms of content provision, and digital advertising.

Content and service personalization

Regarding content, digital providers compete for users' attention, in one or several markets,[145] and there are several strategies that they might choose to compete with. The most relevant ones are by differentiating their content and by using algorithms to make it as relevant as possible for consumers.

Online platforms try to differentiate their content to improve users' engagement, to attract the largest number of possible viewers for the longest amount of time. Some of the content distributed by digital providers can be produced by them or by third parties, and even users. Most online platforms try to differentiate their offers by providing premium or attractive content exclusively.[146] These exclusivity agreements may restrict the possibilities of third parties to provide such content to their audiences, so they can constitute barriers to entry or expansion to other competitors, especially when these agreements are established by dominant market players in a given market.

Nowadays, online content providers might use AI in content production, known as synthetic media[147] —e.g. image synthesis, audio synthesis, speech synthesis, among others—.[148] It has been claimed that synthetic media has some important benefits for

[144] Australia-ACCC (2022). Digital platform services inquiry - September 2022 interim report, p. 34. Available at: https://www.accc.gov.au/system/files/Digital%20platform%20services%20inquiry%20-%20September%202022%20interim%20report.pdf.
[145] OECD (2020). *Competition in digital advertising markets,* p. 29. Available at: http://www.oecd.org/daf/competition/competition-in-digital-advertising-markets-2020.pdf.
[146] In the case of audiovisual content, it has been demonstrated that premium content (e.g. major sport events, exclusive news, and successful recently released films) generates high demand and significant revenues. OECD (2015). *Digital Convergence: Policy and Regulatory Issues,* p. 15. Available: https://one.oecd.org/document/DSTI/ICCP/CISP(2015)2/en/pdf.
[147] Synthetic content is created using a variety of AI techniques, which include: computer-generated imagery (CGI) and natural language processing (NLP).
[148] World Wide Web Consortium (2020). *Synthetic Media Community Group*. Available at: https://www.w3.org/community/synthetic-media/wiki/Main_Page.

content producers, due to the fact that it is automatically created, they can scale up their operations; it can be designed to be delivered across to multiple channels; it can be personalized to customer's preferences; etc. Hence, it can create large volumes of customized content, within reasonable costs.[149] However, it has also been warned that some regulation is needed since it could pose threats to consumers and society, such as propagation of disinformation and "deepfakes".[150]

Besides differentiating their content, online platforms can use AI to enhance user reach, retain consumers attention and engagement. For example, they recommend and prioritize relevant content to users.[151] According to recent research, online platforms use algorithms that process content (face recognition, image filters, language translation, audio transcription, among others) and algorithms that propagates content (content recommendation, content moderation, notifications, trends, among others). Narayan et. al. (2023) explain that recommendation algorithms (recommender systems) play a critical role in the success of online platforms, since the more they can engage a user with their content, the more time they will spend on the digital platform,[152] and so the higher the audience that a digital platform can reach for advertising purposes. (See Annex 4 for more information on how a recommender system works.)

Research suggests that recommendation systems increase user engagement.[153] In this regard, the use of algorithms could explain why some content is viewed more than others. For example, Guinaudeau et al. (2022) quantified that for YouTube the top 20% of an account's videos get 73% of the views, and an account's most viewed video is on average 40 times more popular than its median video.[154]

Digital advertising

Regarding digital advertising, once online platforms have captured consumer's attention, they then monetize this attention by selling digital spaces. Starting from 2017, global expenditure on digital advertising has outstripped television advertising expenditure[155] each year.[156] Hence, digital advertising has been an increasingly key revenue source for many digital platforms.

For advertisers, one of the main advantages of digital advertising is the potential to personalize advertising at great scale, in real time. This type of advertising has been referred as "Online Behavioral Advertising", which makes use of user's data —age, gender, location (in real time), education level, interests, sexual preferences, online shopping behavior, and online history—.[157]

Nowadays, most digital advertising spaces are traded in real time, through bidding processes that are designed to allocate and post ads as quickly as a user scrolls down

[149] Techsense (2023). *Synthetic Content: What is it?*. Available at: https://techsense.lu/news/synthetic-content-what-is-it.
[150] van der Sloot, V. and Wagensveld, Y. (2022). "Deepfakes: regulatory challenges for the synthetic society". *Journal of Computer Law & Security Review*, Volume 46. Available at: https://doi.org/10.1016/j.clsr.2022.105716.
[151] Kaur, H. (2023). Adapting to Social Media Algorithms for Better Reach. The Social Perception, 9th Edition. Available at: https://www.linkedin.com/pulse/adapting-social-media-algorithms-better-reach-hargun-kaur
[152] Narayanan, A. (2023). *Understanding Social Media Recommendation Algorithms*. Available at: https://knightcolumbia.org/content/understanding-social-media-recommendation-algorithms.
[153] Dujeancourt, E. and Garz, M. (2023). "The effects of algorithmic content selection on user engagement with news on Twitter." *The Information Society*, Available at: https://www.tandfonline.com/doi/full/10.1080/01972243.2023.2230471.
[154] Guinaudeau, B. Munger, K. and Votta, F. (2022). *"Fifteen Seconds of Fame: TikTok and the Supply Side of Social Video". Computational Communication Research*, *4*, pp. 463–485. Available at: https://computationalcommunication.org/ccr/article/view/114.
[155] However, different trends might apply to different economies. A key difference is the relevance of household's and mobile internet penetration, the higher the proportion of penetration the higher the level of investment in digital advertising.
[156] Slefo, G. (2017). *Desktop, Mobile Ad Revenue Surpasses TV for the First Time*. Available at: http://adage.com/article/digital/digital-ad-revenue-surpasses-tv-desktop-iab/308808/.
[157] Boerman, S. C., Kruikemeier, S., and Zuiderveen-Borgesius, F. J. (2017). "Online Behavioral Advertising: A Literature Review and Research Agenda." *Journal of Advertising*, Vol. 46 (3), pp. 363-376. Available at: https://doi.org/10.1080/00913367.2017.1339368.

a webpage or access an app. For this, digital advertising is provided through a complex supply chain. On the extremes, there are (i) advertisers and (ii) digital providers —whom provide digital advertising spaces on their apps or websites—. Between them there are technological intermediaries, from the supply side and the demand side, which are known collectively as AdTech.[158] Also, other players that may participate are: data brokers, who collect information from different digital sources, classify, and sell profiles of customers to different players; ad networks, which group together either digital providers or advertisers; among others.

As in the case of content, online platforms might apply different algorithms or weigh data from consumers and advertisers differently, in order to present ads to consumers. For example, YouTube's webpage explains that the ad selection process is designed to deliver the right ad to the right customer at the right time, Google filters ads candidates based on: frequency of capping, advertiser exclusions (preventing two advertisers with competing businesses from showing up on the same page), chooses advertising with the highest historical click-through rate, among others.[159]

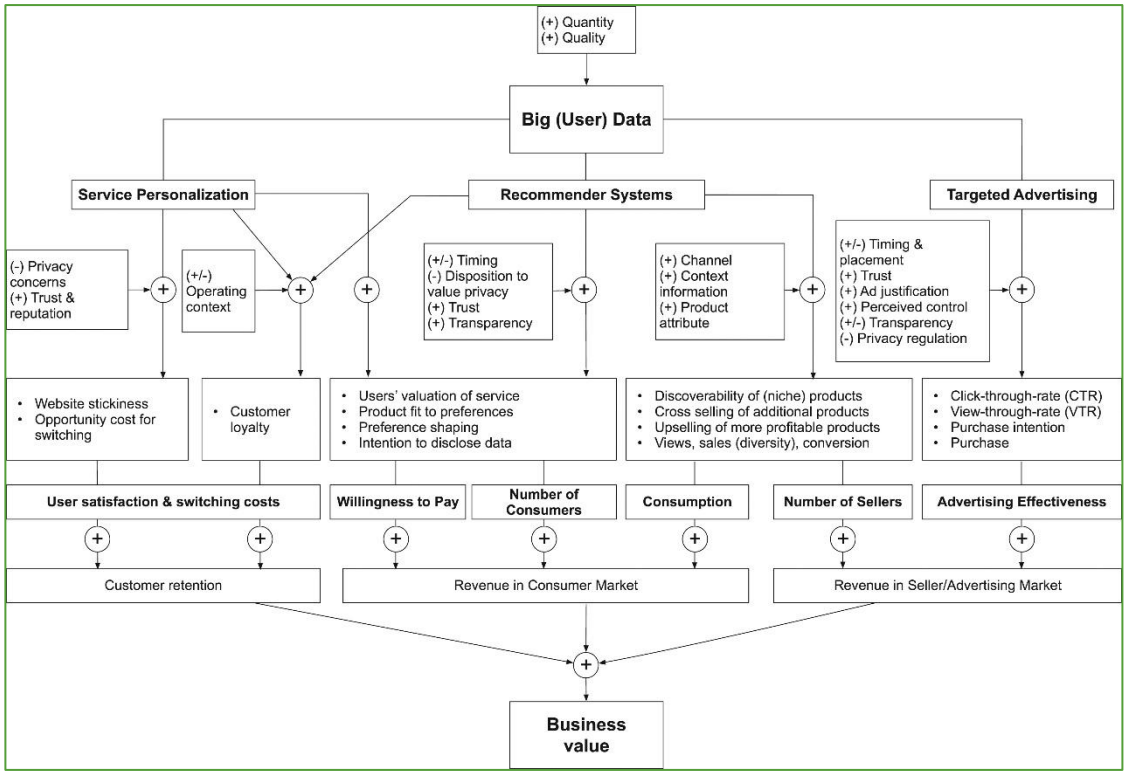
Regarding competition concerns, several competition authorities have pointed out that very few digital players participate along all the supply chain of the AdTech. In particular, it has been demonstrated that Google, through its parent company Alphabet Inc., and Facebook, through its parent company Meta Inc., both operate a fully integrated AdTech services. Also, both of them use its multiple consumer-facing applications to create a unique data set of consumer profiles that underpins their targeted online advertising. Consequently, advertising on Facebook and Google has been claimed to being "unavoidable" or a "must have" due to the scale and reach of its social network platforms and web search services, and given their access to highly detailed consumer data.[160]

Business value creation

According to Fast, Schnurr and Wohlfarth (2023), online platforms' business value is generated along different paths and in different forms. In particular, data-driven business value comes from: (i) improved customer retention, (ii) increased revenue in the consumer market, and (iii) increased revenue on other market sides. The following figure highlights the relevant moderating factors that influence the effectiveness of service personalization, recommender systems, and targeted advertising in generating business value.

[158] In particular, (i) on the supply side: digital providers Ad Servers and Supply Side Platforms; (ii) on the demand side: Demand Side Platforms and Advertisers Ad Servers.
[159] Google (2023). *Ad selection white paper*. Available at: https://support.google.com/admanager/answer/1143651?hl=en.
[160] OECD (2020). *Competition in digital advertising markets,* pp. 25-39. Available at: http://www.oecd.org/daf/competition/competition-in-digital-advertising-markets-2020.pdf.

Figure 5. *Online platforms business value creation*



Source: Fast, Schnurr and Wohlfarth (2023).[161]

3.2.1.4 Concerns for online safety

Users can benefit from the provision of online platforms, in particular for "zero-price", since they can access content, services and information. However, some concerns have been identified in policy areas, such as: competition, privacy and online safety —e.g. misinformation, filtering bubbles, among others—. Hence, some jurisdictions are regulating digital platforms considering competition and online safety concerns.

Dissemination of Illegal or harmful content, democratic and plurality concerns

Online harms encompass various dimensions, including harm in content production and distribution, as well as harm in content consumption. In particular, the following:[162]

- **Harm in the production of content**: where a person is physically harmed, and the abuse is recorded or streamed in order to create online material.
- **Harm in the distribution of content**: resharing hateful comments about a minority group reinforces stereotypes towards the underrepresented group, perpetuating biases and inflicting further harm on these individuals.
- **Harm in the consumption of content:** where a person is negatively affected as a result of viewing illegal, age-inappropriate, potentially dangerous or misleading

[161] Fast, V., Schnurr, D., and Wohlfarth, M. (2023). "Regulation of data-driven market power in the digital economy: Business value creation and competitive advantages from big data". *Journal of Information Technology*, Vol *38*(2), 202–229. Available at: https://doi.org/10.1177/02683962221114394.
[162] World Economic Forum (2023). *Toolkit for Digital Safety Design Interventions and Innovations: Typology of Online Harms*, p. 5. Available at: https://www.weforum.org/reports/toolkit-for-digital-safety-design-interventions-and-innovations-typology-of-online-harms/.

content. Online harms can also occur as a result of online interactions with others (contact) and through behavior facilitated by technology (conduct).

In the case of content diffusion and plurality, it has been explained that digital platforms could intentionally or unintentionally, through their algorithms, promote content that lead to higher reach between users and, consequently, profit margins, but has the power to propagate fake news, misinformation and even harmful or illegal content.

For example, echo chambers might arise because by 'filtering' content, consumers might be exposed to engaging content which is potentially harmful or disinformation, and in the presence of a lack of competitive constraints, consumers could not discipline the digital provider by leaving the platform.[163]

Also, the plurality of content could be jeopardized, since *"there are growing concerns that citizens' media diets are less diverse due to content being highly personalized and reflecting fewer, and more polarized, points of view"*.[164] This constitute a societal harm that affects access and exposure to a diversity of content which has been explained to be central in the making of a resilient democracy.

Regarding synthetic content, new harms to consumers have been identified, such as:[165]

i) Synthetic content could be used to create fake news, propaganda and other forms of disinformation that lead to challenges in authentication.

ii) Audiences may find it difficult to trust the authenticity of content and audiences could potentially be harmed if it is not apparent they are watching footage that is a 'Deepfake'.

iii) Audiences could mistake 'Deepfake' footage of a real person in a way that could result in unfairness to them or potentially unwarrantably infringe on their privacy.

Competition policy concerns

Some online platforms play a very important role in the provision of one or several digital services in which they participate (e.g. when they have integrated ecosystems or are vertically integrated).

Digital players that have attained positions of market power have commercial incentives to maintain those positions, either through legitimate means (innovation, better services, more privacy to consumers, etc.) or anti-competitive practices. In particular, when these digital platforms constitute a bottleneck to access consumers they can have the incentives to implement policies to restrict competition.[166] For example, limiting competitors' content diffusion, choosing technical standards to prevent competitors from accessing their platforms or tying, acquiring actual or potential competitors, among others.

[163] United Kingdom-OFCOM (2019). *Online market failures and harms: an economic perspective on the challenges and opportunities in regulating online services,* p. 30-33. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0025/174634/online-market-failures-and-harms.pdf.
[164] Government of Canada (2022). *Diversity of Content Online*. Available at: https://www.canada.ca/en/canadian-heritage/services/diversity-content-digital-age.html.
[165] United Kingdom-OFCOM (2023). *Synthetic media (including deepfakes) in broadcast programming*, p. 1. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0028/256339/Note-to-Broadcasters-Synthetic-media-including-deepfakes-.pdf.
[166] Ezrachi, A. and Stucke, M.E. (2022). *The Darker Sides of Digital Platform Innovation*. Available at: https://www.networklawreview.org/ezrachi-stucke/

Absent effective competitive constraints, large digital platforms may have the ability and incentive to engage in anti-competitive conducts, such as: exclusionary and exploitative, which pose risks for competition and online safety.

Regarding exclusionary conducts, competition authorities have found the following:

i) **Self-preferencing**: to affect rivals' abilities to compete, a digital platform gives unduly preferential treatment to its own products/services over those of third-party providers. This conduct also affects consumers whenever the quality of the third-party products/services are better, or cheaper, compared to those self-provided by the digital platform, or when given higher prices of advertising translate into higher final prices. In digital advertising, self-preferencing has been related to the following practices: (i) use of discriminatory terms and conditions of access; (ii) low transparency over fees and verification; (iii) limiting, delaying or denying interoperability to platform, among others.[167] Also, digital platforms with market power could reduce the discoverability of rivals' content, or give preferable treatment in search rankings to content providers with whom they have exclusivity agreements.

ii) **Tying**: a digital platform with market power may exclude or hinder its competitors by tying a service in which it has market power to a product or service it provides in a related market. While firms may assert that there are legitimate justifications for some tying conduct, such as promoting efficiency, or addressing security or privacy concerns, such claims need to be carefully considered by authorities, since tying conducts can harm competition in various ways, including, for example, by limiting access to users and/or reducing the ability of rivals to gain sufficient scale to profitably and/or effectively compete in that market.

iii) **Barriers to switching and multi-homing**: by making consumers' switching more difficult digital platforms aim to protect their market position. By restricting consumers' ability to switch to products or services that better meet their needs, digital platforms with market power impede new entrants to reach consumers and compete on the merits. Digital platforms with market power could, for example, choice interphase architectures and dark patterns to restrict fair comparisons, and limit multi-homing and switching.

iv) **Transparency**: the lack of sufficient transparency and enough information over the prices, terms of service, and key functions undertaken by digital platforms, has a detrimental effect on investment and purchasing decisions from firms and consumers. In the case of ad tech, a lack of transparency around auction prices and exchange fees, as well as vertical integration, strong position across the supply chain and the 'must have' nature of certain digital services, has raised concerns from competition authorities.[168]

v) **Exclusivity and price parity clauses**: When digital platforms hold market power, platform's business users and consumers can face significant bargaining

[167] United Kingdom-CMA (2020). *Online platforms and digital advertising market study*. *Final Report*, pp. 306-308. Available at: https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf.

[168] For example, the ACCC found that Google has limited publishers' ability to link certain bid data files, this has limited publishers' ability to compare the performance of supply-side platforms for auctions in Google's publisher ad server; and has also limited information to advertisers' so they do not have the ability to independently assess the performance of Google's demand-side Platform. Furthermore, the authority has stated that Google has the ability and incentive to retain 'hidden fees' in its auctions. Australia-ACCC (2021). *Digital Advertising Services Inquiry Final Report*, pp. 143, 149-150, 152, 151-156. Available at: https://www.accc.gov.au/publications/digital-advertising-services-inquiry-final-report.

imbalances and usually must accept the service on whatever terms it is offered. For example, exclusivity clauses imposed by an intermediary platform service provider with market power would require its business users to only offer their products or services through its platform. This would restrict business users' ability to offer their products or services on competing intermediary platforms. Depending on the clause, it might even restrict the business user from selling its products or services through any other sales channel.

Regarding exploitative conducts, these could include the following:

i) For consumers, abuse of significant market power could involve degradation of the quality of the services provided by the digital platform, either through, for example, more advertising, higher costs or unfair terms, such as being required to provide more data to access services (worse privacy terms or more information being collected).

ii) For business users, this may involve paying forced fees, higher commissions or advertising fees, or unfair trading practices.

Exploitative conduct may ultimately lead to lower consumer choice whenever it reduces the incentives for businesses to enter, improve and innovate, or may be passed onto consumers in the form of higher prices or diminished quality for products or services.

3.2.1.5 International experience to improve online safety

European Union

The Digital Service Act[169] (DSA), which entered into force on November 2022, regulates the obligations of digital services that act as intermediaries in their role of connecting consumers with goods, services, and content. Its main objective is ensuring a safe, predictable and trusted online environment, addressing the dissemination of illegal content online and the societal risks that the dissemination of disinformation or other content may generate, and within which fundamental rights are effectively protected and innovation is facilitated.

The DSA is an asymmetric regulatory regime, i.e. larger intermediary platforms with wider societal influence are subject to stricter regulations. In particular, the regulated services include:

i) **Intermediary services offering network infrastructure**: (i) mere conduit services: Internet access providers (such as internet exchange points, wireless access points, virtual private networks) and DNS services; (ii) caching services: content delivery networks, reverse proxies and content adaptation proxies, etc; and (iii) hosting services, such as cloud and webhosting services.

ii) **Online platforms (including online search engines[170]):** defined as platforms which bring together sellers and consumers, for example: online marketplaces, app stores, collaborative economy platforms and social media platforms. Hence, online platforms include services that not only store information provided by the

[169] European Union-European Parliament (2022). *Digital Services Act*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065.

[170] Intermediary service that allows users to input queries to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found.

recipients of the service at their request, but also disseminate that information to the public[171] at the request of the recipients of the service.

iii) **Very large online platforms** (VLOPs) and **Very large online search engines** (VLOSEs) whom pose particular risks in the dissemination of illegal content and societal harms. In particular, those with at least 45 million average monthly active users/recipients within the EU.

The obligations of different online players match their role, size and impact in the online ecosystem, and it follows a tiered regulatory system. This implies that a basic common set of rules applies to all intermediary services, including network infrastructure services. A second tier of additional rules applies to all the hosting services. A third tier of additional obligations applies only to hosting service providers which disseminate users' content to the public. A fifth tier of additional obligations applies only to the VLOPs and VLOSEs which are designated by the European Commission —by September 2023 the European Commission designated **six gatekeepers**[172] **Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft** under the Digital Markets Act[173] (DMA), and 22 core platform services[174] provided by gatekeepers have been designated[175]—.

Table 1. Key obligations under the DSA

	Intermediary services	Hosting services	Online platforms	VLOP/VLOSE
Transparency reporting	●	●	●	●
Requirements on terms of service due account of fundamental rights	●	●	●	●
Cooperation with domestic authorities following orders	●	●	●	●
Points of contact and, where necessary, legal representative	●	●	●	●
Notice and action, obligation to provide information to users		●	●	●
Reporting criminal offences		●	●	●
Complaint and redress mechanism and out of court dispute settlement			●	●
Trusted flaggers			●	●
Measures against abusive notices and counter-notices			●	●
Bans on targeted adverts to children and those based on special characteristics of users			●	●
Transparency of recommender systems			●	●
User-facing transparency of online advertising			●	●

[171] The concept of 'dissemination to the public', as used in the DMA, entail the making available of information to a potentially unlimited number of persons, meaning making the information easily accessible to recipients of the service in general without further action by the recipient of the service providing the information being required, irrespective of whether those persons actually access the information in question. DSA, paragraph: 14.

[172] Three main quantitative criteria that create the presumption that a company is a gatekeeper as defined in the DMA: (i) when the company achieves a certain annual turnover in the European Economic Area and it provides a core platform service in at least three European Union Member States;(ii) when the company provides a core platform service to more than 45 million monthly active end users established or located in the European Union (EU) and to more than 10,000 yearly active business users established in the EU; and (iii) when the company met the second criterion during the last three years. The DMA also empowers the Commission to conduct market investigations to: (i) designate companies as gatekeepers on qualitative grounds; (ii) update the obligations for gatekeepers when necessary; (iii) design remedies to tackle systematic infringements of the Digital Markets Act rules.

[173] The DSA was promulgated along with the DMA a complementary regulation that aims to promote competition by preventing biggest online companies from abusing their market power. European Parliament (2022). *Digital Markets Act*. Available at: https://digital-markets-act.ec.europa.eu/index_en.

[174] According to the DMA, core platform services are: online intermediation services such as app stores, online search engines, social networking services, certain messaging services, video sharing platform services, virtual assistants, web browsers, cloud computing services, operating systems, online marketplaces, and advertising services.

[175] European Union-European Commission (2023). *Digital Markets Act: Commission designates six gatekeepers*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_4328.

	Intermediary services	Hosting services	Online platforms	VLOP/VLOSE
Risk management obligations and crisis response				●
External & independent auditing, internal compliance function and public accountability				●
User choice not to have recommendations based on profiling				●
Data sharing with authorities and researchers				●
Codes of conduct				●
Crisis response cooperation				●

Source: European Commission (2022).[176]

The European Commission has powers to directly supervise VLOPs and VLOSEs. Additionally, each Member State will have to designate a domestic Digital Services Coordinator, who will supervise other entities in scope of the DSA as well as VLOPs and VLOSEs for non-systemic issues. The domestic coordinators and the European Commission will cooperate through a European Board of Digital Services. This EU-wide cooperation mechanism will be established between domestic regulators and the Commission.

United Kingdom

In September 2023, the Online Safety Bill[177] was signed off by the Houses of Parliament and became law on October 2023 after receiving Royal Assent. The Bill imposes duties on digital providers that seek to secure (among other things): (i) a higher standard of protection for children than for adults; (ii) protection of users' rights to freedom of expression and privacy; and (iii) transparency and accountability in the provision of internet services.

The services that are regulated by the Bill include: user-to-user services,[178] search services[179] and combined services[180]. In determining what is proportionate for different duties, the Bill considers the following factors: (i) findings of the most recent risk assessments, and (ii) the size and capacity of the provider of the service.

The Online Safety Bill applies to "regulated" Services and Search Services. These services are "regulated" if they have "links" with the UK which means:

- the service has a significant number of UK users or UK users form a target market for the service; and/or
- the service is capable of being used in the UK by individuals and there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the UK.

The following table contains the main duties that providers must compel with, according to the services provided (further details please see Annex 5).

[176] European Union-European Commission (2022). *The Digital Services Act: ensuring a safe and accountable online environment*. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en.
[177] United Kingdom-Parliament (2023). *Online Safety Bill*. Available at: https://bills.parliament.uk/publications/52368/documents/3841.
[178] As defined by the Bill, an internet service by means of which content that is generated directly on the service by a user of the service, or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users, of the service. In: United Kingdom-Parliament (2023). *Online Safety Bill*, p. 14.
[179] As defined by the Bill, an internet service that is, or includes, a search engine. In: United Kingdom-Parliament (2023). *Online Safety Bill*, p. 15.
[180] As defined by the Bill, a regulated user-to-user service that includes a public search engine. In: United Kingdom-Parliament (2023). *Online Safety Bill*, p. 16.

Table 2. Key obligations under the Online Safety Bill

Duties	User-to-user services and search engines
Duties of care	**All services**: illegal content risk assessment; illegal content handling; content reporting; complaints procedures; freedom of expression and privacy; record-keeping and review.
	Children (when services are likely to be accessed by children): children's risk assessments; protections to children's online safety
	Category 1 or 2a: assessments related to adult user empowerment; protect content of democratic importance; protect news publisher content; protect journalistic content.
Cross cutting duties: freedom of expression and privacy	**All services**: When deciding on, and implementing, safety measures and policies freedom of expression and privacy. **Category 1 or 2a**: Impact assessment in the adoption and implementation of the safety measures and policies would have on: users' right to freedom of expression within the law and the privacy of users.
Cross cutting duties: Record-keeping and review duties	**All services**: duty to make and keep a written record of any measures taken or in use to comply with a relevant duty which— (a) are described in a code of practice and recommended for the purpose of compliance with the duty in question, and (b) apply in relation to the provider and the service in question.
Fraudulent Advertising	**Category 1:** A provider of a Category 1 service must operate the service using proportionate systems and processes designed to— (a) prevent individuals from encountering content consisting of fraudulent advertisements by means of the service; (b) minimize the length of time for which any such content is present; (c) where the provider is alerted by a person to the presence of such content, or becomes aware of it in any other way, swiftly take down such content. **Category 2a:** A provider of a Category 2A service must operate the service using proportionate systems and processes designed to— (a) prevent individuals from encountering content consisting of fraudulent advertisements in or via search results of the service; (b) if any such content may be encountered in or via search results of the service, minimize the length of time that that is the case; (c) where the provider is alerted by a person to the fact that such content may be so encountered, or becomes aware of that fact in any other way, swiftly ensure that individuals are no longer able to encounter such content in or via search results of the service.

Source: Online Safety Bill. **Note:** For purposes of presentation only the most relevant duties were included.

United Kingdom's Office of Communication (OFCOM), communications regulator, will be the online safety regulator. OFCOM will put in place detailed codes of practice and guidance to set out the details of the regulatory regime.

OFCOM will be granted a range of enforcement powers including:

- using an expert (at the service provider's cost) to inspect a service provider's systems;
- powers of entry and inspection at a service provider's premises;
- issuing an enforcement notice requiring a service provider to do, or refrain from doing;
- issuing fines of up to GBP18 million or 10% of global revenue;
- criminal sanctions for failing to comply with a requirement of an information notice, including fines and imprisonment for up to two years; and/or
- issuing orders requiring a provider of "ancillary services" to an in-scope service (i.e. a service that facilitates the provision of the regulated service (or part of it) (for example, advertising or credit card services)) to withdraw the ancillary service to the extent that it relates to the relevant service.

It is expected that OFCOM will finalize all relevant codes and guidance in phases from 2024, and it is expected that the regulatory regime will be fully operational until 2025.

Based on preliminary estimations, the number of online service providers subject to regulation could total more than 100,000.[181]

As part of the DRCF, OFCOM and the CMA published a joint statement in which they recognized that there may be some scope for policy synergies, in particular some interventions may promote both competition and online safety. For example, by creating more choice and enabling users to switch more easily, competition interventions can allow consumers or advertisers to choose to engage most with those platforms that are best at keeping them safe or safeguarding their commercial interests.

However, authorities recognized that interventions in one policy area sometimes might create a risk of negative unintended effects in another. The CMA and OFCOM consider important to identify and mitigate such impacts wherever they can, and that the rules set for online services do not impose conflicting requirements. For example, it is possible that interventions which seek to enhance online safety may increase the cost of entry to a market, reducing the ability of start-up firms to enter or compete with existing services. Similarly, some competition interventions may risk worsening online safety if they prevent companies from taking actions that can help to protect users. In those cases, CMA and OFCOM will work together to find the best approach to tackle both policy concerns.[182]

Australia

In 2021, the Australian Parliament approved the Online Safety Act. The regulation includes a range of schemes to keep Australians safe online, including mechanisms to remove seriously abusive and harmful content. The eSafety Commissioner is in charge of its enforcement. The regulation addresses among others the following:[183]

- **Image-based abuse**: administers an image-based abuse scheme which provides a mechanism for Australians to seek the removal of intimate images that have been shared without consent. Victims of this type of abuse are able to contact eSafety directly to seek help.
- **Online Content Scheme**: The Act establishes an Online Content Scheme which is designed to protect consumers, particularly children, from exposure to harmful material. The Online Content Scheme provides a mechanism for members of the public to make complaints to eSafety about illegal or harmful content, and for eSafety to assess these complaints.
- **Child cyberbullying**: eSafety administers a complaints service for Australian children who experience serious cyberbullying. Under the scheme, eSafety can investigate complaints about serious cyberbullying material targeting an Australian child and require its removal.
- **Rapid website blocking arrangements**: to protect Australians from exposure to extremely harmful material such as live-streaming of terrorist attacks. This allows eSafety to respond to online crisis events by requiring internet service providers block access to material depicting, promoting, inciting or instructing in abhorrent violent conduct.

[181] United Kingdom-National Audit Office (2023). *Preparedness for online safety regulation*, p. 9.
[182] United Kingdom-CMA and OFCOM (2022). *Online safety and competition in digital markets: a joint statement between the CMA and Ofcom*. Available at: https://www.gov.uk/government/publications/cma-ofcom-joint-statement-on-online-safety-and-competition/online-safety-and-competition-in-digital-markets-a-joint-statement-between-the-cma-and-ofcom#how-competition-and-online-safety-policies-interact-in-digital-markets.
[183] Australian-Australian Government (2021). *Online Safety Act 2021*. Available at: https://www.legislation.gov.au/Details/C2021A00076.

- **Adult Cyber Abuse Scheme**. eSafety administers a complaints service for Australian adults aged 18 or older who experience seriously harmful abuse online. Under the scheme, eSafety can investigate complaints of serious adult cyber abuse where the platform has failed to respond, and may require its removal.

3.3 Collaboration between competition and regulatory authorities to tackle harms and risks from data collection and analysis

3.3.1 Data

The term "data" can be used to refer to any information or representation of it, often in combination with its storage in a computer.[184] Data can be described based on various characteristics that will determine its value, and with it, the possibility that it may constitute a source of market power, a barrier to competition, or a means to displace other competitors. In general terms, data is an intangible asset with various economic characteristics that are described below:

i) **Nonrivalry, but excludable**. Data can be used by various economic agents at the same time, for different purposes, without there being a functional loss in the original data.[185] According to some authors, this means, on one hand, that data is subject to increasing returns to scale, and, on the other, through property rights, or privacy rights, certain data can be only used by some firms.

ii) **Economies of scope**. The data collected by a company can be reused for other purposes, such as the development of new products or applications. This is called “economies of scope in data reuse”.[186] In other words, economies of scope are achieved when a data set is combined with other data.

iii) **Economies of scale in use**. Some authors point out that there are diminishing returns and refer to the Netflix recommendation algorithm, which is almost as accurate after using a few tens of thousands of data as when it uses a few million data.[187] In contrast, other authors argue that the use of data in certain artificial intelligence applications can exhibit increasing returns.[188] According to these perspectives, it seems that the returns may be increasing or decreasing depending on the complexity of the data processing required.

iv) **Informational externalities**. Once a company has accumulated a certain amount of data, it can be used to predict the behavior of users outside the sample.

v) **High investment costs and low marginal costs**. Data collection and analysis typically means that companies must invest in hardware, software, and the development of specific capabilities (for example, data science and analytics skills) and processes to collect and maintain data.

[184] France-Autorité de la Concurrence and Germany-Bundeskartellamt (2016). *Report on Competition Law and Data*, p. 4. Available at: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf;jsessionid=3731EEFE925E4649143C37AC7F5FDFBD.1_cid390?__blob=publicationFile&v=2.

[185] Martens, B., De Streel, A., Graef, I., Tombal, T., & Duch-Brown, N. (2020). “Business-to-Business data sharing: An economic and legal analysis.” *JRC Digital Economy Working Paper* 2020-05, p. 9 Available at: https://joint-research-centre.ec.europa.eu/system/files/2020-07/jrc121336.pdf: and Jones, C.I. and Tonetti, C. (2020). “Nonrivalry and the Economics of Data”, *American Economic Review*, Vol. 110, No. 9. Available at: https://www.aeaweb.org/articles?id=10.1257/aer.20191330.

[186] Martens, B. (2020). “An economic perspective on data and market power”. *JRC Digital Economy Working Paper*, 2020 pp. 6 -7. Available at: https://joint-research-centre.ec.europa.eu/system/files/2021-02/jrc122896.pdf.

[187] Antuca, A. (2021). *If data is so valuable, how much should you pay to access it?* Oxera. Available at:: https://www.oxera.com/insights/agenda/articles/if-data-is-so-valuable-how-much-should-you-pay-to-access-it/.

[188] Agrawal, A., Joshua, G., & Avi, G. (2018). “Prediction machines: The simple economics of Artificial Intelligence.” *Harvard Business Review Press*.

3.3.2 The importance of data for providers of digital services

Data is one of the most important intangible assets for the provision of digital services. For digital providers data triggers two types of feedback loops that reinforce each other:[189,190]

i) **User feedback loop**: data is used to improve the quality of digital services. Digital providers who have access to better databases –in terms of volume, velocity, veracity, and variety– on their customers can improve the quality of their services, which then attracts more users, creating a virtuous cycle.

ii) **Monetization feedback loop**: by using consumer data, digital platforms can improve their services; for example, targeted advertising, for which they can obtain additional funds; these funds can be used to invest in the quality of their main service and could lead to gaining more users, reinforcing the virtuous cycle.

Figure 6. Feedback loops

Source: OECD (2019).

Additionally, the Stigler Center's Report emphasized that the returns to more dimensions and types of consumer data may be increasing. Hence, it has warned that digital providers have no incentives to stop accumulating new pieces of data, entrenching incumbents with large datasets *vis-à-vis* entrants with smaller databases.[191] Also, access to more data can improve a digital provider's opportunity to enter into the provision of new services. In other words, by reusing data gathered in the context of one digital service undertakings may provide new services based on it.[192]

Nonetheless, it has been claimed, that while the initial costs of collecting data can sometimes be substantial, the marginal cost of sharing it, either through copying or providing access to it, is typically very low. Furthermore, once collected, sharing data does not, therefore, decrease its value for the initial collector (i.e., is a 'non-rivalrous' good).[193]

[189] Furman, J, et. al. (2019). *Unlocking digital competition: Report of the digital competition expert panel*. Report prepared for UK Treasury, p. 33. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.

[190] OECD (2016). *Big data: Bringing competition policy to the digital era*, p. 10. Available at: https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf.

[191] Stigler Centre (2019). *Committee for the Study of Digital Platforms. Market Structure and Antitrust Subcommittee: Report*, pp. 24-25, 27-28. George J. Stigler Center for the Study of the Economy and the State. The University of Chicago Booth School of Business. Available at: https://research.chicagobooth.edu/-/media/research/stigler/pdfs/market-structure---report-as-of-15-may-2019.pd.

[192] France-Autorité de la Concurrence and Bundeskartellamt (2016). *Competition Law and Data*, p. 10. Available at: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2.

[193] United Kingdom-CMA and ICO (2021). *Competition and data protection in digital markets joint statement*, p. 12. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/987358/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf.

However, when incumbents (i.e., well-established digital firms) can hoard data and impede its sharing, data can act as an entry barrier and lead to market outcomes with limited competition and reduced social benefits.[194]

3.3.3 Market power in digital markets from data collection

Following the previous reasoning, since data is a relevant asset for the provision of digital services, it could confer a form of unmatchable advantage on the incumbent providers.

Whenever new entrants or small participants cannot access or collect and process similar data —in terms of volume, velocity, veracity, and variety— to provide equivalent digital services as the incumbents, this would make successful rivalry less likely.[195]

On the one hand, the Japan Fair Trade Commission explained *"[d]igital platform enterprises are collecting and accumulating vast amounts of personal data as result of offering «free» services or networks, and while it would not be technically impossible for new entrants to collect similar data, doing so would be economically unrealistic for new entrants under the present circumstances."*[196]

On the other, as explained by Rubinfeld and Gal, *"those* [firms] *who enjoy more portholes from which to gather data, who have a substantial database to which they can compare new data, or who possess unique data synthesis and analysis tools, may enjoy a competitive comparative advantage."*[197]

Furthermore, if a digital platform also operates as a competitor to its business users, it could have a unique advantage regarding the knowledge and data it holds about its rival business users and their customers. For example, the European Commission antitrust case against Google asserted that Google restrained the ability of third parties —such as advertisers, publishers, or competing online display advertising intermediaries— to access data about user identity or user behavior, hence, data was only available to Google's advertising intermediation services.[198]

In this regard, in recent competition cases, competition authorities have assessed the importance of data on whether a digital firm holds substantial market power; in particular they have considered the following aspects. First, the type and characteristics of the data that an undertaking may hold. Second, whether if it is exclusively accessed and its replicability, i.e., if such that data can act as a barrier to entry or expansion. Third, the extent of the economic advantage that the data provides to the undertaking, which includes assessing its business model in a relevant market and potentially in several adjacent markets.[199]

---

[194] Carriere-Swallow, Y. and Haksar, V. (2019). *The Economics and Implications of Data: An Integrated Perspective*, p. 1. International Monetary Fund, *Departmental Papers*, Vol. 2019, Issue 013. Available at: https://www.elibrary.imf.org/view/journals/087/2019/013/article-A001-en.xml.

[195] For example, Farboodi et. al. (2019) modelled data as an intangible asset that reduces uncertainty about random variables that are relevant for production. In particular, firms accumulate data which affects competition dynamics, as it increases the skewness of the firm size distribution. On the one hand, large firms generate more data and invest more in active experimentation; while, small data-savvy firms can overtake more traditional incumbents, if they can use data efficiently; however, to do so they have to overcome financial costs from the initial phase of operation. Farboodi, M., Mihet, R., Philippon, T., and Veldkamp L. (2019). "Big Data and Firm Dynamics." *AEA Papers and Proceedings*, Vol. 109: 38-42. Available at: https://www.aeaweb.org/articles?id=10.1257/pandp.20191001.

[196] Japan Fair Trade Commission (2017). *Report of Study Group on Data and Competition Policy*, p. 15. Available at: https://www.jftc.go.jp/en/pressreleases/yearly-2017/June/170606_files/170606-4.pdf.

[197] Rubinfeld, D. and Gal, M. (2016). "Access to barriers to big data", p. 342. *Arizona Law Review*, Vol. 59. Available at: https://arizonalawreview.org/pdf/59-2/59arizlrev339.pdf.

[198] European Commission (2021). *AT.40670 Google - Adtech and Data-related practices*. Press release. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3143;
https://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_AT_40670.

[199] Li, L. (2019). "Data and market definition of Internet-based businesses." In: *Competition and Regulation in Network Industries*, *20*(1), pp. 54–85. Available at: https://journals.sagepub.com/doi/full/10.1177/1783591719840132.

Economic literature has explained that data can constitute a barrier to entry and expansion in digital markets. In the following lines, they are summarized the most relevant ones for the purposes of this document:[200]

- **Technological barriers**: If data can only be collected from unique access points, this could reduce or limit its replicability. For example, through certain digital providers, specific activities, or through specific apps or devices. The FTC noted that *"vertical integration of ISP services with other services like home security and automation, video streaming, content creation, advertising, email, search, wearables, and connected cars permits not only the collection of large volumes of data, but also the collection of highly-granular data about individual subscribers"*.[201]
    - **Economies of scale and scope**: The cost of putting in place infrastructure for data collection and analysis may generate high fixed costs; and the actual and potential uses of data could enhance the economies of scope or limit them. For example, how certain data could be used to enter into another market, provide a new service, trigger feedback loops.
    - **Network effects**: Data-driven network effects can create a demand-side technologically based barrier to entry. This is the case when having more users attracts more users, or if data and the new information (from these users) can be used to improve the quality of services, then entry of new firms that do not have such data might be difficult.
- **Behavioral (strategic conducts)**: Data collectors may implement strategic conducts to prevent data to be shared with their competitors. For example, contractual exclusive access to a unique source of data may create entry barriers in the form of input or outlet foreclosure; access prices and conditions set by the data owner for granting access to his data; digital providers might disable one another's data-gathering mechanisms; increase switching costs of data sharing; among others.
- **Legal**: Legal barriers are often justified by broader welfare goals, such as privacy, however they also carry costs in the form of limiting access to data by different providers. Legal barriers can create direct as well as indirect barriers to the collection of data (either self-collection or transfer from another data collector).

Hence, the competitive advantage that big digital players can gain from the combination of economies of scale, scope and network effects can lead markets to 'tip' in favor of one or few incumbents. In this case, competitive constraints would mostly come from entrants who may displace incumbents by launching new or improved services. However, where barriers to entry are too high, incumbents can gain and exploit market power in a way which cannot be eroded, at least not sufficiently promptly, by potential entrants.[202]

[200] Rubinfeld, D. and Gal, M. (2016). "Access to barriers to big data", pp. 339-363. In: *Arizona Law Review*, Vol. 59. Available at: https://arizonalawreview.org/pdf/59-2/59arizlrev339.pdf.
[201] FTC (2021). *A Look at What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers*, p. 33. Available at: https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.
[202] United Kingdom-OFCOM (2019). *An economic perspective on the challenges and opportunities in regulating online services*, p. 19. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0025/174634/online-market-failures-and-harms.pdf.

In summary, whenever access to data can constitute a barrier to entry or expansion, it can lead to a lack of competitive pressure from new entrants within those markets.[203] So, competition authorities are advised to analyze whether the access to data can constitute or reinforce a digital provider's dominant position.

3.3.4 Case studies of merger and anticompetitive conducts related to data

The following are cases of mergers and anticompetitive conducts where competition authorities have analyzed the role of data in digital markets.[204]

Mergers and acquisitions

A merger could raise competition concerns if the combination of databases of the merging firms, would make it impossible for competitors to replicate the information extracted from it. In these cases, the acquirer might engage in a merger in order to get access to better or differentiated data. For example, this could motivate acquisitions where there are non-horizontal overlaps between undertakings or where the value or market share of the acquired firm is relatively low. In these cases, the primary motivation of the merger is the value and scarcity of the data is and how the combined databases would improve the merging firm's comparative advantage.

Also, mergers between digital platforms who participate in upstream or downstream markets along the same supply chain, or separate upstream or downstream markets, would be motivated to engage in foreclosure conducts. For example, where a dominant digital provider would acquire new firms to guarantee its access to data.

The following box presents Theories of Harm (ToH) in merger cases related to data access, which have been analyzed by competition authorities in different economies.

Box 1. Merger cases where ToH were analyzed regarding data access

Given the prominence of data in digital mergers, competition authorities are advised to analyze if a separate relevant market for data shall be defined and the effects of merged data in potential competition and market dynamics.[205] In appropriate cases, competition authorities could consider if the merged data fulfills the so-called 'nonrivalry' characteristic, otherwise if data can act as a barrier to entry or expansion.[206]

In Apple/Shazam (2018), the European Commission investigated two main ToH related to data. First, whether the transaction would give Apple access to commercially sensitive information about competing music streaming platforms, in particular Spotify. Second, whether the data collected by Shazam could have been used to improve existing functionalities or to offer additional functionalities, on digital music streaming apps. The Commission compared Shazam's data to other available datasets on users of digital music services based on the so-called "four V's" –volume, velocity, veracity, and variety–, and concluded that Shazam's data was not more comprehensive than other datasets available in the market.[207]

[203] Furman, J, et. al. (2019). Op. Cit. p. 34.
[204] Autorité de la Concurrence and Bundeskartellamt (2016). *Competition Law and Data*, p. 10. Available at: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2.
[205] In particular, the Competition Bureau of Canada stated in a discussion paper that when data is good to be traded "the closeness of competition between two firms selling data will depend on the extent to which customers view their data products as substitutable". Canada Competition Bureau (2018). *Big data and innovation – Implications for competition policy in Canada*, p. 12. Available at: https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/Big-Data-e.pdf/$file/Big-Data-e.pdf.
[206] Please for more information refer to:
- Graef, I. (2015). Market definition and market power in data: The case of online platforms. World Competition, 38(4), 473-505.
- Valdani Vicari, et. al. (2021). Support study accompanying the evaluation of the Commission Notice on the definition of relevant market for the purposes of Community competition law, Final Report, p. 90. Available at: https://ec.europa.eu/competition-policy/system/files/2021-06/kd0221712enn_market_definition_notice_2021_1.pdf.

[207] European Commission (2018). *Commission Decision of 6 September 2018 in Case M.8788 – Apple/Shazam*. Available at: https://ec.europa.eu/competition/mergers/cases/decisions/m8788_1279_3.pdf.

Exclusionary conducts

A digital provider with a dominant position in one or several markets could have the ability and incentive to incur in anticompetitive conducts, in the access and use of data, if by doing so it might reinforce its dominant position. For example,[208]

- **Refusal to access**: in the case where the data owned by a digital incumbent is truly unique and that there is no possibility for competitors to obtain the data they need to perform their services elsewhere, then refusal to its access could be claimed to be anticompetitive if it reinforces its dominant position.[209]
- **Discriminatory access to data**: vertical integration can entail discriminatory access to strategic information with the effect of distorting competition. In particular, if it is able to restrict information that their competitors operating on the marketplace get about the transactions they are involved in.
- **Exclusive contracts**: preventing rivals from accessing data through exclusivity provisions with third-party providers or foreclosing opportunities for rivals to procure similar data by making it harder for consumers to adopt their technologies or platforms.[210]
- **Tied sales and cross-usage of datasets**: data collected on a given market could be used by a company to develop or to increase its market power on another market in an anti-competitive way.

3.3.5 Abuse of dominance in the collection of data, breaches to privacy law and competition law

As explained before, dominant digital platforms have the ability and incentives to collect vast amounts of information regarding their consumers. Hence, some jurisdictions are analyzing where competition and privacy law intersect, particularly for the collection and use of personal data of individuals.

In this regard, some economies have stressed the importance to analyze the potential consequences for consumers derived from the data gathering capabilities from dominant digital platforms. These could arise due to asymmetries of power between some digital providers and consumers.

Nowadays, there are proposals for competition authorities, on how to implement their attributions having into account privacy law, which fall in the following categories:[211]

i. Evaluate privacy as a non-price dimension of competition and examine whether a transaction (merger) would reduce the merged firm's incentives to compete on consumer privacy protections.

---

[208] Autorité de la Concurrence and Bundeskartellamt (2016). *Competition Law and Data*, pp. 15-25. Available at: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2.

[209] As OFCOM has explained that there are specific conditions that must be fulfilled to determine that data can be regarded as an essential facility: a) there is a refusal to supply; b) the requested party is dominant on an upstream 'market' for the supply of the input and the anticompetitive effects of the refusal arise on a second, downstream, 'market'; c) the input in question is essential for competition on the second market, in the sense that it cannot be duplicated or can only be duplicated at an uneconomic cost; d) the refusal to deal would eliminate competition on the second market; e) at least in the case of IP rights, the refusal to deal prevents the emergence of a new product for which there is consumer demand or otherwise limits 'technical development'; and f) no objective considerations justify the refusal to deal. In United Kingdom-OFCOM (2022). *Data, Digital Markets and Refusal to Supply*, Economic discussion paper series, issue number 6, pp. 11. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0028/248950/Data,-Digital-Markets-and-Refusal-to-Supply.pdf.

[210] European Commission (2010). *"Google. Case 38740"*. Available at: http://europa.eu/rapid/press-release_IP-10-1624_en.htm?locale=en.

[211] Ohlhausen, M. K. and Okuliar, A. (2015) "Competition, Consumer Protection, and the Right (Approach) to Privacy", pp. 134-136. *Antitrust Law Journal*, No. 1 (2015). Available at: https://www.ftc.gov/system/files/documents/public_statements/686541/ohlhausenokuliaralj.pdf.

ii. Analysis between the costs and benefits of consumer protection against the impact on competition, for the implementation of laws.

iii. Hold companies accountable under the antitrust laws to the extent those companies mislead or deceive consumers about data collection practices that helped the companies achieve or maintain monopoly power.

iv. Look for possible harms to privacy from transactions or conducts beyond just analyzing the harm to privacy as an existing dimension of competition.

Each one of these would work regarding specific cases, so they could be understood as complementary.

A prominent example is the Case C-252/21 Meta Platforms vs Bundeskartellamt, in which the German competition authority issued a decision against Meta Platforms based on Section 19 of the German Competition Act, according to which Meta Platforms abused its dominant position on the German market for social networks imposing abusive business terms to the users of the service available at «facebook.com».

The highlights of the case are explained in the following box.

Box 2. Bundeskartellamt vs Facebook, Case C-252/21[212]

According to the investigation of the Bundeskartellamt, Facebook was found to be the dominant company in the German market for social networks for private users, and its scope of action was not sufficiently controlled by competition. In its dominance analysis, it was asserted that Facebook had excellent access to competitively relevant data (Facebook, WhatsApp, Instagram, Oculus and Masquerade), highly relevant for competition as a social network and for highly personalized advertising, given its data policy.

Regarding its data policy, the authority found that it was in violation of the European Union General Data Protection Regulation (GDPR) data protection, to the detriment of both private users and competitors. It allowed Facebook to collect user and device-related data, from sources outside of Facebook and to merge it with data collected on Facebook. Hence, it was in breach of the data protection legal bases established in the GDPR, its collection and merging capabilities could not be justified outside the social network.

In the ruling, the Bundeskartellamt concluded that Facebook's data policy:

i. **Violation of GDPR as a manifestation of market power**: this conduct was only possible because of its market dominance and competitors did not behave similarly;
ii. **Forcing Privacy terms and conditions:** users cannot protect their data from being processed for a large number of sources, i.e. they cannot decide autonomously on the disclosure of their data; and
iii. **Distorting Competition**: it impedes competition because Facebook gains access to a large number of further sources by its inappropriate processing of data and their combination with Facebook accounts.

In the Case C-252/21, the European Court of Justice reach a final decision in which it concluded that competition authorities can rule on the compliance or non-compliance of the undertaking with the GDPR in the context of a decision on an abuse of a dominant position.[213] Among the reasons considered, Advocate General Rantos, of the European Court of Justice, issued an opinion regarding the use of European Union General Data

[212] Bundeskartellamt (2019). *Decision under Section 32(1) German Competition Act (GWB) - Public version -*. Available at: http://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf%3F__blob%3DpublicationFile%26v%3D5.

[213] Curia (2023). Case C-252/21 Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Limited, formerly Facebook Ireland Ltd., Facebook Deutschland GmbH v Bundeskartellamt. Available at: https://curia.europa.eu/juris/documents.jsf?num=C-252/21.

Protection Regulation (GDPR) as a benchmark to assess a competition infringement. The Advocate General stated that:

> *"a competition authority, within the framework of its powers under the competition rules, may examine, as an incidental question, the compliance of the practices investigated with the rules of that regulation, while taking into account any decision or investigation of the competent supervisory authority on the basis of said regulation, informing and, where appropriate, consulting that authority."*[214]

In the decision, the Court of Justice also recognized that parameters of competition in the digital economy involves significant use of personal information, such that cooperation between competition and privacy enforcement authorities is necessary for the authorities to discharge their regulatory functions. More importantly, the Court noted that, under the Treaty on the Functioning of the European Union, authorities have a duty to engage in sincere cooperation with counterparts when an issue raises concerns in multiple regulatory spheres.

In this regard, it is expected to set a precedent on how privacy law breaches could be considered for the enforcement of competition law.

3.3.6 Collaboration between competition and regulatory authorities to address concerns on data collection

Consumer's data collection, and its potential uses, is a matter that mainly concerns to authorities with statutory duties on data protection and privacy. In some economies, these statutory duties are safeguarded by a single authority and other authorities (competition, cybersecurity, telecommunications, consumer protection, etc.) are required by law to collaborate with them. In other jurisdictions, given the importance to safeguard consumers' rights in digital markets, different authorities have decided to collaborate even when legal provisions do not require them to do so. Hence, there is a growing interest to understand how effective collaboration between agencies can be performed.

Cross-regime coordination between agencies and/authorities is not new, and has been done through legal mechanisms, institutional mechanisms, or a combination of both. The following explanation follows the work of CERRE based on the European Union experience, and could be useful for some economies.[215] Nonetheless, different domestic frameworks could result in different options for economies.

In the first case, legislators could create a system of priorities to deal with potential overlaps between statutory duties of agencies and/or authorities. The system of priorities could work following: (i) General/specific laws articulation[216] or (ii) Principal/accessory relation.[217]

---

[214] Curia (2022). Opinion of Advocate General Rantos, on Case C-252/21 Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Limited, formerly Facebook Ireland Ltd., Facebook Deutschland GmbH v Bundeskartellamt. Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany. Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=265901&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=344793.

[215] CERRE (2022). *Improving EU Institutional Design.* Available at: https://cerre.eu/wp-content/uploads/2022/01/20220117_CERRE_Report_Improving-EU-Institutional-Design_Final.pdf.

[216] A general rule (law) would apply fully regardless of the sector; when a specific regulatory regime applies then it should not contradict the general regime (unless otherwise stated in law).

[217] In the case of composite services which are potentially covered by different laws, instead of applying all those different legal regimes, only the one pertaining to the principal component would apply, leaving aside the law applicable to the accessory component.

In the second case, the authorities would need to collaborate and establish institutional mechanisms for working together this could be done on a case-by-case basis or a general framework of collaboration. In particular, collaboration can work for:

i. Consultation: authorities consult each other before reaching a decision, each authority remains competent to apply its own regulatory framework. This can promote an agreed position on the nature of the infringement and the remedies.

ii. Joint case work: authorities might agree to share information (subject to proper procedural safeguards); work jointly to design remedies; and in the monitoring of remedies.

iii. Joint technical policy making: authorities could work on common regulatory document and guidelines which may then be a useful common basis when each authority must decide individual cases.

Nonetheless, frictions between competition and regulatory objectives could appear, hence a coordination between both is necessary.

In the following two boxes examples of collaboration between authorities are presented for the case of data.

Box 3. Italy's Market Study on Big Data[218]

The Italian Competition Authority (AGCM), the Communications Authority (AGCom) and the Data Protection Authority (DPA) elaborated a Market Study on Big Data.

Through the Study, the three authorities concluded that *"the challenges posed by the digital and data-driven economy require a sound implementation of ex ante and ex post assessments' synergies in order to safeguard privacy, competition, consumer welfare and pluralism."*

The Study concludes that the challenges posed by the digital economy cannot be effectively tackled without a common approach and it explores how synergies between the three institutions, equipped with complementary tools, can be effectively achieved whilst respecting each other's missions. From the information gathered they provided some policy recommendations on how to tackle the issues raised by data privacy and protection law and competition law:[219]

- **Reduce information asymmetries between digital corporations/platforms and their users**: (i) Consumers should be informed about the use of their data but also on the extent their data are needed for the functioning of the service; (ii) during purchase decisions and data transfers, users are aware of the connection between the consent necessary for the functioning of the app and the request of further authorization following data transfer; (iii) the entrance of new data intermediaries, vested with stronger contractual position regarding data commercial exploitation, should be encouraged.
- **Pursue the goal of consumer welfare with the aid of antitrust law tools**: (i) Digital economy features require to strike a balance between the risk of discouraging innovation and the risk of underenforcement; (ii) through competition law tools, consumer welfare goals should be pursued not only by considering conduct based on prices and quantities but also on other parameters such as quality, innovation and fairness.

[218] For further information check:
- Italian Competition Authority (2020). *Consumer data rights and competition – Note by Italy*. Available at: https://one.oecd.org/document/DAF/COMP/WD(2020)33/en/pdf; and
- Italy-ITA, AGCOM and DPA (2019). *Study n. IC53 - BIG DATA, decision n. 28051*. *Guidelines and policy recommendations*. Available at: https://en.agcm.it/dotcmsdoc/pressrelease/Big%20Data_Guidelines%20and%20policy%20recommendations.pdf.

[219] In this box it is provided a summary of the most relevant recommendations addressed in the study, the criteria for its selection considered the scope of the virtual session and specific actions to be followed by authorities. For the full set of recommendations please see: ITA, AGCOM and DPA (2019). Op. Cit.

- **Reform merger control regulation**: (i) Potential competition: competition authorities should be allowed to examine concentrations that do not meet the thresholds which trigger the obligation to give prior notification but that are still capable of reducing potential competition (such as the acquisition by major digital firms of innovative start-ups – i.e. "killing acquisitions"); (ii) introduce an evaluation standard grounded on the "Substantial impediment to effective competition criteria".
- **Facilitate data portability and data mobility between platforms**: bearing in mind the importance to respect individual data protection rights, competition law enforcement could lead towards additional portability and mobility. Data portability should be extended –besides GDPR– through the adoption of measures which both enhance data access competition and strengthen consumer protection.

Box 4. Framework of collaboration between UK's CMA and ICO[220]

The Information Commissioner's Office (ICO) and the Competition and Market Authority (CMA) prepared a joint statement where they presented the areas that they would work on.

The joint statement first clarifies which are the legal duties of each authority, and then explains the synergies and potential tensions that could arise from an uncoordinated action.

Synergies:

- **User choice and control**: (i) Effective competition can enable stronger privacy protections, and weak competition can undermine those protections; (ii) effective data protection can also support competition as rival companies seek to build consumer trust and confidence in the way that their personal data is used.
- **Standards and regulations to protect privacy**: Well-designed regulation and standards that preserve individuals' privacy and place individuals in control of their personal data can serve to promote effective competition and enhance privacy. This can be done by: (i) ensuring that competitive pressures help drive innovations that genuinely benefit users, rather than encouraging behavior that undermines data protection and privacy rights; (ii) competitive pressures can be harnessed to drive innovations that protect and support users.
- **Data-related interventions to promote competition**: Ensuring a level playing field between participants, for example restricting access to data, or limiting the ability to combine and integrate datasets, for platforms with market power.

Potential tensions:

- **Data access interventions**: Data access between undertakings should be limited to what is necessary and proportionate, sharing should be designed and implemented in a data protection-compliant way, and related processing operations should be developed in line with the principles established in law (data protection by design and by default). Also, they should not result in a facilitation of unlawful or harmful practices.
- **Risk of interpreting data protection law in an anti-competitive manner**: There is a risk of data protection law being interpreted by large integrated digital businesses in a way that leads to negative outcomes in respect of competition, e.g. by unduly favoring large, integrated platforms over smaller, non-integrated suppliers.

4 Recommendations

This section summarizes the economic and policy considerations discussed in the previous sections and includes some possible ways to address the consumer protection, privacy and competition issues that arise.

[220] United Kingdom-CMA and ICO (2021). Competition and data protection in digital markets joint statement, pp. 18-26. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/987358/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf.

4.1 Recommendations on "Consumers' protection: interplay between Consumer Protection and Competition Enforcement in Digital Markets –Artificial intelligence and Dark Patterns–"

- Economies are advised to carefully address potential individual and social harms that could arise from the unfair, deceptive, anticompetitive or abusive use of AI systems. Where *ex ante* AI systems regulations are deemed appropriate, they could potentially include aspects such as: rights of individuals and communities to notice and explanation, deployment of safety and effective systems to address harms, encourage developers, deployers and uses of AI systems to take proactive and continuous measures to protect individuals and communities from algorithmic discrimination and to use and design systems in an equitable way.
- Regulations that address potential harms and risks from the unfair, deceptive, anticompetitive or abusive deployment and use of AI should consider which are the different actors that participate in the supply chain of these systems, in order to consider all the relevant actors and assign liabilities, and effective measures to address the potential harms arising from the use and implementation of AI systems.
- Competition, privacy and other regulatory authorities are advised to collaborate between them in order to consider the specific characteristics of the economics of AI systems and particularly to adequately prevent harms by digital providers that hold substantial market power. This collaboration would foster that regulations do not have unduly adverse effects on innovations and market entry, and it would also foster sharing experiences, expertise and knowledge between them.
- Economies are advised to study how dark patterns affect consumer decisions and may consider issuing regulations or guidelines that address the use of dark patterns, including definitions and prohibitions flexible enough to address evolving practices and examples of practices that may constitute prohibited dark patterns.
- Issue regulations that explicitly prohibit the use of dark patterns (in general and not only in specific cases), define in legislation or guidelines which practices could be considered as dark patterns, and analyze and study how the use of dark patterns affects consumers' decisions.
- Promote international collaboration to adopt a common terminology, definitions and classifications, on dark patterns, to enhance international enforcement cooperation.

4.2 Recommendations on "Online Safety"

- Online safety regulations should promote the effective exercise of rights of individuals, and should also include effective ways through which online platforms must comply and protect these rights.
- Economies should consider defining which are the types of content that should qualify as illegal and harmful, and which are the specific measures that online platforms should use to avoid in the dissemination of such content.

- Authorities are advised to consider how online platforms operate in their economies, identify which are the biggest online players by reach between users, and to consider the possibility of using asymmetric regulation to impose higher risk controls to those online providers with higher reach.
- All relevant authorities are advised to collaborate in order to prevent the imposition of unnecessary regulatory burdens on new players, or to those with lower reach. Collaboration is deemed necessary to prevent ineffective regulatory frameworks that could affect competition.

4.3 Recommendations on "Collaboration between competition and regulatory authorities to tackle harms and risks from data collection and analysis"

- Competition and regulatory authorities are advised to consider how the gathering and use of data has an impact on the business model and revenue generation of digital providers. This implies to analyze how feedback loops between data collection and business value operate and which would be the best ways to address potential bottlenecks and entry barriers in the collection of data.
- Competition and regulatory authorities are advised to consider the possibility of imposing terms on data collection that are consistent with privacy regulations on digital providers with sufficient market power to harm competition.

  or

  Competition and regulatory authorities are advised to analyze whether one or several digital providers with market power could use such power in detriment of competition conditions, as well as affecting the protection of personal data/privacy of users by imposing terms on data collection and/or processing that are consistent with personal data protection/privacy regulation.
- Competition authorities are advised to collaborate with privacy regulators, and where deemed needed and appropriate, to implement adequate regulatory measures, that could foster data sharing, without jeopardizing personal data/privacy protection.
- Collaboration between authorities is deemed necessary to contribute in the harmonious implementation of different public policy objectives.

Annexes

Annex 1

The following box presents examples from industries and sectors using AI systems, and some concerns that have been identified.

Box. AI applications in some sectors and industries

Examples of industries using AI systems and some challenges for consumer protection that have been identified:

Banking and finance: Banks are using various AI systems to detect fraudulent activity, solutions to provide customer service, identify abnormalities, and prevent credit card fraud. AI systems are used to learn and recognize patterns in historical data and forecast how they will recur in the future. Nonetheless, some concerns are rising, in particular: (i) bias in AI decisions, (ii) the ability to explain the rationale of its decisions, (iii) their robustness (particularly with respect to cyber threats and privacy), and (iv) their potential impact on financial stability.[221]

Media: AI systems can be useful to provide better advanced search services, content creation, automated captioning, content moderation, incentivize consumer retention, among others.[222] However, AI systems could be used to create and propagate disinformation *"which poses serious threats to society, as it effectively changes and manipulates evidence to create social feedback loops that undermine any sense of objective truth"*.[223]

Telecommunications and Internet of Things: 5G, the latest technological standard for wireless telecommunication networks, and future telecommunications networks will make use of AI systems. It is expected that with the use of AI systems companies will be able to optimize network operations, increase energy efficiency and reduce operating costs.[224][225] The combination of AI systems, 5G and the linking of billions of devices through the Internet of Things (IoT) will enable new capabilities in transport, entertainment, industry, and public services, and much more. However, it is expected that given the diversity of services/applications and the growing number of connected things envisaged in the networks will open up new and increasingly broad cyber threats, posing security and privacy risks.[226]

Health care: Devices, such as Fitbit or iWatch, are used to collect data related to heartbeats, sleep patterns, calories burnt by users, among others. This information can be analyzed by AI systems for disease diagnosis. Also, complex algorithms can be used to imitate human discernment for analyzing healthcare and medical data, among others.[227] Despite its benefits, some challenges that have been identified by the Government Accountability Office of the United States include: (i) real-world performance across diverse clinical settings and in rigorous studies; (ii) AI technologies need to be integrated into clinical workflows; and (iii) regulatory gaps need to be addressed to provide clear guidance for the development of adaptive algorithms.[228]

Education: AI could be useful for automated marking software, content retention techniques, monitoring the psychological, mental and physical well-being of students, including the academic part and their all-round developments. Some challenges that have been identified are: (i)

[221] Boukherouaa, E. B., AlAjmi, K., Deodoro, J., Farias, A., and Ravikumar, R. (2021). "Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance" *International Monetary Fund Departmental Papers*, Vol. 24, A001. Available at: https://www.elibrary.imf.org/view/journals/087/2021/024/article-A001-en.xml.

[222] VSN Video Stream Networks (2022). *Artificial Intelligence real applications for Broadcast & Media Industries*. Available at: https://www.vsn-tv.com/en/artificial-intelligence-applications-broadcast-and-media/.

[223] University of Stanford (2022). *2021 Report, SQ10. What are the most pressing dangers of AI?* Available at: https://ai100.stanford.edu/2021-report/standing-questions-and-responses/sq10-what-are-most-pressing-dangers-ai.

[224] International Telecommunications Union (ITU) (2019). *New ITU standard to introduce Machine Learning into 5G networks*. Available at: https://aiforgood.itu.int/new-itu-standard-to-introduce-machine-learning-into-5g-networks/.

[225] Morocho-Cayamcela, M.E. and Lim, W. (2018). "Artificial Intelligence in 5G Technology: A Survey". In *2018 International Conference on Information and Communication Technology Convergence (ICTC)*. pp. 860-865. Available at: https://ieeexplore.ieee.org/document/8539642.

[226] Benzaïd, C. and Taleb, T. (2020). "AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?" In *IEEE Network*, Vol. 34, No. 6, pp. 140-147. Available at: https://ieeexplore.ieee.org/document/9186438.

[227] In particular, for 5G the AI systems will allow base stations to predict what kind of content users nearby may request, dynamic allocation of frequencies in self-organized LTE dense small cell deployments, automatically reduce latency, detect anomalies/faults/intrusions, among others. Davenport T, and Kalakota R. (2019). "The potential for artificial intelligence in healthcare." *Future Healthcare Journal*. Vol. Jun;6(2), pp. 94-98. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6616181/.

[228] United States-Government Accountability Office (2022). *Artificial Intelligence in Health Care: Benefits and Challenges of Machine Learning Technologies for Medical Diagnostics*. Available at: https://www.gao.gov/products/gao-22-104629.

balancing human and computer decision making; (ii) avoid surveillance and protect students' privacy; (iii) AI systems decisions require to be inspectable, explainable and overridable;[229] and (iv) AI systems should be designed and tested to be unbiased and ethical.

[229] United States-Office of Educational Technology (2023). *Artificial Intelligence and the Future of Teaching and Learning*. Available at: https://www2.ed.gov/documents/ai-report/ai-report.pdf.

Annex 2

In this annex it is presented a general overview of risks that could arise for consumers and final users when AI providers do not implement adequate controls to: (i) the decision-making process; (ii) biases in the results; and (iii) privacy and data gathering.

Data. It has been identified that there are circumstances where personal data from consumers is obtained and processed without the direct participation or knowledge of consumers. This could be, either because they were not informed or because data subjects provide their consent for the reuse of their data but they may not always understand what this means in practice. In either case, consumers are not fully aware that an AI system is processing their personal data, in these cases consumers are also unable to seek redress for any harms that may have occurred as a result of that processing and they may not even be aware that they are being harmed.

Privacy risks. As AI systems require an active strategy to keep a steady stream of new and useful information flowing (data pipeline), they can have incentives to collect more data than necessary to provide a specific digital service. As explained by the Federal Trade Commission (FTC), AI systems can incentivize increasingly invasive forms of commercial surveillance.[230] Also, privacy experts are claiming that privacy law should also consider the following harms: physical, economic, reputational and psychological.[231]

Liability within AI supply chain. Algorithmic processing often involves multiple parties, each playing a different role in the journey from the creation of an algorithm to its deployment. In particular, one party may collect data, another may label and clean it, and another still may use it to train an algorithm. Hence, the number of players involved in algorithmic supply chains could lead to confusions regarding who is accountable for their proper development and use.[232]

Cybersecurity. Experts have warned that there are several ways that AI systems could be undermined. One of these is by poisoning training data, resulting in models with lower levels of accuracy. Cyber criminals could, for example, seek to corrupt the training data used to build a detections models or by deploying "adversarial examples".[233] Also, algorithms can be manipulated to leak sensitive information, for example, "model inversion", where personal information can be inferred about individuals who are featured in training datasets.[234]

Right to the explanation of a decision. Since most AI systems involve complex sets of ML there is no straightforward way to map out the decision-making process, creating "black boxes". Once AI systems process the data and take a decision or perform an action, programmers, managers, shareholders or even authorities, might not be able to accurately understand the linkage between an input (data) and an output (for example, profiling or an automated decision), and how the decision-making process has been done to get to a

[230] United States-Federal Trade Commission (FTC) (2022). *Combatting Online Harms Through Innovation*. Available at: https://www.ftc.gov/reports/combatting-online-harms-through-innovation.
[231] Keats Citron, D. and Solove, D.J. (2021). "Privacy Harms". In *Boston University Law Review*. Vol 102. Available at: https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf.
[232] Cobbe, J. and Singh, J. (2021). *Artificial Intelligence as a Service: Legal Responsibilities, Liabilities, and Policy Challenges*. *Computer Law & Security Review*. Volume 42, September 2021. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0267364921000467.
[233] Belfer Center for Science and International Affairs (2019). *Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It*. Available at: https://www.belfercenter.org/publication/AttackingAI.
[234] United Kingdom-ICO (2019). *Privacy attacks on AI models*. https://ico.org.uk/about-the-ico/news-and-events/ai-blog-privacy-attacks-on-ai-models/.

certain result.[235] Hence, it has been warned that in some cases *"it may not be possible to truly understand how a trained AI program is arriving at its decisions or predictions."*[236]

For this reason, AI systems have raised some concerns among authorities and academics:

> *"The implications of this inability to understand the decision-making process of AI are profound for* [legal] *intent and causation tests*, *which rely on evidence of human behavior to satisfy them.* […] *This also means that little can be inferred about the intent or conduct of the humans that created or deployed the AI."*[237]

Biases. AI systems have been subject to some critiques regarding potential biases in their outcomes. AI systems require an active strategy to keep a steady stream of new and useful information flowing (data pipeline);[238] however, this data could not always be statistically representative of the whole population of interest. In this regard, it has been warned that AI systems can suffer from data biases, which emanates from unrepresentative or incomplete training data or the reliance on flawed information that reflects historical inequalities. Hence, *"[i]f left unchecked, biased algorithms can lead to decisions which can have a collective, disparate impact on certain groups of people even without the programmer's intention to discriminate."*[239] For example, when AI systems are used to generate profiles of users[240] and for "automated decision-making" if biases are not correct then these could lead to harms for consumers, for example underrepresented of marginalized communities and persons.

Also, the United States' National Institute of Standards and Technology (NIST) has identified that AI could lead to biases from: (i) measurement and metrics to support testing and evaluation, validation, and verification, and (ii) human factors, including societal and historic biases within individuals and organizations.[241]

[235] United States-FTC (2018). *Transcript of FTC Hearings Session #7: Competition and Consumer Protection in the 21st Century - Day 2*, Comments of Nichola Petit, Professor of Law, U. of Liege, Belgium, pp. 107-108. Available at: https://www.ftc.gov/system/files/documents/public_events/1418693/ftc_hearings_session_7_transcript_day_2_11-14-18_0.pdf.
[236] Bathaee, Y. (2018). "The Artificial Intelligence Black Box and the Failure of Intent and Causation", p. 892. *Harvard Journal of Law & Technology*, Vol. 31, Num. 2, Spring 2018. Available at: https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf.
[237] Bathaee, Y. (2018). Op Cit., pp. 892-893.
[238] AI needs two classes of data: fixed- size data assets that can be used to train the models for generic tasks, and data that is actively generated by the system as it experiments and improves performance.
[239] World Economic Forum (2022). *Open source data science: How to reduce bias in AI*. Available at: https://www.weforum.org/agenda/2022/10/open-source-data-science-bias-more-ethical-ai-technology/.
[240] For example, what led a user to visit the site (referrals), how effective the user experience is within the site (web analytics), and the nature of who is using the site (audience segmentation). In some cases, the data collected is used to dynamically adapt content (personalization) or advertising presented to the user (targeted advertising). In: W3C (2019). *Tracking Preference Expression (DNT)*. Available at: https://www.w3.org/TR/tracking-dnt/.
[241] United States-NIST (2022). *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*. NIST Special Publication 1270. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf.

Annex 3

Based on academic research, some of the most effective dark patterns are presented in the following table. [242]

Table. Taxonomy of dark patterns

Category			Type	Explanation
Information Asymmetry	Active Misleading Actions	Misleading Information	Testimonials of Uncertain Origin	Misleading users by providing them false, confoundin deceiving, or exaggerated information
			Scarcity	Misleading users by providing them false, confoundin deceiving, or exaggerated information
			Friend Spam	Misleading users by providing deceiving information
			Fake Countdown Timers	Misleading users by providing them fraudulent information
			Limited-time Messages	Misleading users by providing them deceiving or exaggerated information
		Misleading Presentation	Trick Questions	Misleading users through wording
			Misdirection (Visual Interference)	Misleading users by using visual interference
	Passive Misleading Omissions	Hiding Information	Price Comparison Prevent	Misleading users by withholding clear and comprehensible price information
		Delaying Provision	Hidden Costs	Delaying price information provision
Free Choice Repression	Undesirable Imposition	Pressure Imposing	Pressured Selling (Repeat Popup Dialogs or Confirm Shaming)	Imposing pressure on users through repeated inquirie or wordings that make users experience guilt or sham
		Forced Acceptance	Sneak into Basket	Compelling consumers to accept the uninvited produ by directly placing the products in their shopping carts
			Privacy Zuckering (Easy to Register)	Compelling consumers to accept the undesirable subscription by using tricks that thrust them towards subscriptions
			Forced Continuity (Hidden Subscription)	Compelling consumers to continue the subscription b renewing their membership subtly
			Bait and Switch	Compelling users to accept a particular arrangement manipulatively navigating them away from their origin objective regardless of their willingness
			Disguised Advertisement	Compelling users to view an advertisement by manipulatively navigating them away to a location tha they did not expect to reach, regardless of their willingness
	Undesirable Restriction	Restricting Specific Users	Forced Action (Enrol to Access, Pay to Skip, and Accept to Access)	Restricting unpaid or unsubscribed users from option such as content access or skipping of advertisements
		Restricting Specific Actior	Roach Motel (Hard to Cancel)	Making specific actions such as unsubscribing more complicated than needs to be

Source: Leiser, M. and Yang, W-T. (2022).[243]

The following box presents some examples of how dark patterns are used in mobile apps, cell phones and by Internet Service Providers (ISPs).

[242] Luguri, J., Strahilevitz, L.J. (2021). "Shining a Light on Dark Patterns". In *Journal of Legal Analysis*, Vol. 13, Issue 1, pp. 43–109. Available at: https://academic.oup.com/jla/article/13/1/43/6180579; Graßl, P. Schraffenberger; H., Zuiderveen Borgesius, F., Buijzen, M. (2021). "Dark and Bright Patterns in Cookie Consent Requests", *Journal of Digital Social Research*, Vol. 3/1, pp. 1-38. Available at: https://jdsr.se/ojs/index.php/jdsr/article/view/54; United Kingdom-Competition & Markets Authority (2022). *Discussion Paper, Online Choice Architecture: How digital design can harm competition and consumers*, pp. 18-19. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf; and OECD (2022). Op. Cit. pp. 10-11.

[243] Leiser, M. and Yang, W-T. (2022). "Illuminating manipulative design: From 'dark patterns' to information asymmetry and the repression of free choice under the Unfair Commercial Practices Directive". In Artitificial Intelligence and the Media: Reconsidering Rights and Responsibilities. Edward Elgar Publishing Ltd., p. 8-32. Available at: https://osf.io/preprints/socarxiv/7dwuq/. From European Commission, Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F. Liva, G., Lechardoy, L. et al. (2022). Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation: final report, p.90. Publications Office of the European Union. Available at: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418.

Box. Dark patterns used in mobile apps, cell phones and by ISP providers to subvert privacy options

The FTC conducted two studies on dark patterns and found the following evidence. In general, both studies found that digital providers use interfaces to maximize information collection and sharing, such as using default settings to make consumer data collection difficult to avoid, even when such collection is unnecessary. Evidence points to the greater effectiveness of dark patterns on mobile devices or smaller screens, where information is less prominent.[244]

- **Default options for location data**: Some providers set up as the default data collection option the one which maximizes geographical tracking. Location data has been demonstrated to be is extremely valuable for companies, since it can reveal sensitive details about consumers including: where they live and work, sexual orientation, political and religious affiliations, health habits, etc.[245] In particular, it has been found that Google's Android phones portray "location tracking" in such a way that consumers would turn it on.

  The FTC sued data broker Kochava, Inc., related to its sale of consumer location data. The FTC alleged in its complaint that Kochava sold geolocation data from hundreds of millions of mobile devices—data that can be used to trace the movements of individuals to and from sensitive locations, including reproductive health clinics, places of worship, and domestic violence shelters, among others.[246]

- **Privacy practices of major ISPs**: the FTC Report on Internet Service Providers' found the following evidence: (i) ISP's highlighted their preferred choice while less favorable alternatives were greyed out; (ii) most favorable privacy choices for consumers were not presented as a first choice, instead they were buried or hidden, which forced them to scroll and click on tabs and sub-tabs in order to review and change their privacy preferences; (iii) unclear toggle settings could confuse consumers into selecting a privacy setting they did not intend, among others.

- **Collection of mobile numbers**: Digital providers collect mobile numbers, however they are seldom actually needed for the provision of an online service, they do it, in most cases, because it's another way they can identify users and for target advertising.[247]

Source: FTC (2022), pp. 15-17, and FTC (2021), pp. 39-41.[248]

[244] Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). "(Un)informed Consent: Studying GDPR consent notices in the field", *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (CCS '19), pp. 973- 990. Available at: https://doi.org/10.1145/3319535.3354212.

[245] Kantor, M. (2021). *What Is the Business Value of Location Data?* Available at: https://www.esri.com/about/newsroom/publications/wherenext/what-is-the-business-value-of-location-data/.

[246] United States-FTC (2022). FTC v. Kochava, Inc., Case No. 2:22-cv-377 (D. Idaho)- FTC Press Release, FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations. Available at: https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-trackspeople-reproductive-health-clinics-places-worship-other.

[247] Heddings, L. (2018). *Facebook is Using Your Phone Number to Target Ads and You Can't Stop It*. Available at: https://www.howtogeek.com/367766/facebook-is-using-your-phone-number-to-target-ads-and-you-can%E2%80%99t-stop-it/.

[248] United States-FTC (2021). *What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers*. FTC Staff Report. Available at: https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.

Annex 4

According to academic and journalistic research, digital platforms, and particularly those that provide "zero-price" services, mostly[249] use the following recommendation algorithms or a combination of these:[250]

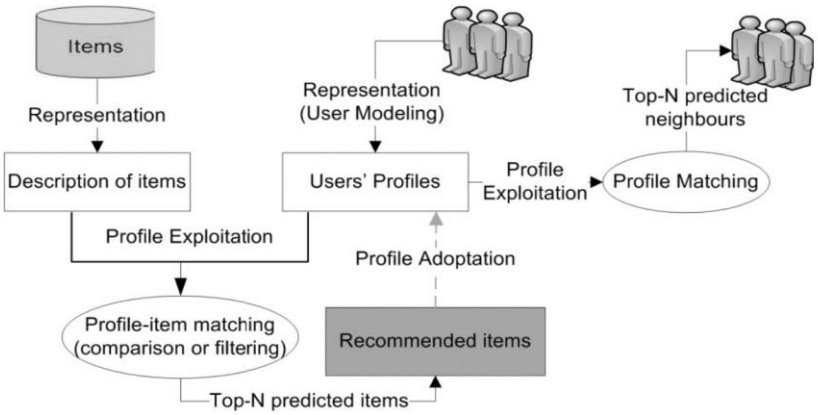
i) **Collaborative-Filtering Recommendation Systems**: evaluates products using users' ratings (explicit or implicit), this algorithm develops a database of the user's preferences. Active users will be mapped against this database to reveal the active user's neighbors with similar preferences. First, the algorithm locates similar users to the target user; second, the algorithm obtains rates for the content from similar users to the active user, and then use them to produce recommendations. Collaborative filtering can generate models that help users discover new interests.

ii) **Content-Based Recommendation Systems**: these are build using a user profile to predict ratings on unseen items. Successful content-based methods utilize tags and keywords, hence content-based filtering can be employed where the features' values can easily be extracted.

iii) **Demographic-Based Recommendation Systems**: This system employs user attributes as demographic data to obtain recommendations (i.e., recommend products based on age, gender, language, etc.). The key advantage is that they are fast and straightforward in obtaining results using a few observations.

The following figure presents a general model of a typical recommendation system.[251]

Figure. General model of a Recommendation system



Source: Khusro, S., Ali, Z., Ullah, I. (2016).[252]

As shown in the figure, a recommender system uses information from: (i) all the possible items (contents) that may be recommended to a user; and (ii) all users for which the system makes recommendations. The system makes recommendations to users by maximizing a utility function that matches the information of the user to all other users

[249] Other recommendation algorithms used are: Utility-Based Recommendation Systems and Knowledge-Based Recommendation Systems, please refer to Fayyaz, Z., et. al. (2020) for further details.
[250] Fayyaz, Z., Ebrahimian, M., Nawara, D., Ibrahim, A., Kashef, R. (2020). "Recommendation Systems: Algorithms, Challenges, Metrics, and Business Opportunities." *Applied Sciences*. Vol 10 (21). Available at: https://doi.org/10.3390/app10217748.
[251] Each item is described in the recommendation system according to its own features and properties, these can be updated as the users interact with the system. For each user, a user profile is created and updated according to new information —e.g. personal information, items visited, rated, purchased and downloaded—, hence, digital providers that have access to more consumer data, have a competitive advantage.
[252] Khusro, S., Ali, Z., Ullah, I. (2016). "Recommender Systems: Issues, Challenges, and Research Opportunities", pp. 1180-1181. In: Kim, K., Joukov, N. (eds). *Information Science and Applications* (ICISA) 2016. *Lecture Notes in Electrical Engineering*, Vol. 376. Springer, Singapore. Available at: https://link.springer.com/chapter/10.1007/978-981-10-0557-2_112.

who are “similar” to her, and the characteristics of the items that have been liked by the user and other users similar to her.

Narayanan (2023) explains that while all recommendation algorithms behind the digital platforms seek users’ engagement, they differ on *how* they optimize it, i.e. the information signals (data) they use and the computational techniques involved.[253] For example, evidence shows that the following digital platforms apply different optimizations to improve engagement:

i) **Facebook**: optimizes for “Meaningful Social Interactions”, a weighted average of Likes, Reactions, Reshares, and Comments.[254]

ii) **YouTube**: between 2012 and 2016, optimized expected watch time (i.e. how long the algorithm predicts the video will be watched). If a user sees a video in their recommendations and doesn’t click on it, the watch time is zero; if they click on it and hit the back button after a minute, the watch time is one minute.[255]

iii) **Netflix**: originally optimized for suggesting movies that the user is likely to rate highly on a scale of one to five.

[253] Narayanan, A. (2023). Op. Cit.
[254] Wong, J.C. (2018). “Facebook Overhauls News Feed in Favor of ‘Meaningful Social Interactions”. *The Guardian*, Jan. 11, 2018. Available at: https://www.theguardian.com/technology/2018/jan/11/facebook-news-feed-algorithm-overhaul-mark-zuckerberg.
[255] Covington, P., Adams, J., Sargin, E. (2016). *Deep Neural Networks for YouTube Recommendations*. Available at: https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/45530.pdf.

Annex 5

According to the Online Safety Bill, the main risk assessments that digital providers must fulfil include the following aspects:

i) **Illegal content risk assessment**, includes an analysis on: the user base; the level of risk users of the service may encounter, taking into account algorithms used by the service, and how easily, quickly and widely content may be disseminated by means of the service; the level of risk of the service to be used for the commission or facilitation of a priority offence; level of risk of functionalities of the service that can facilitate the presence or dissemination of illegal content or the use of the service for the commission or facilitation of a priority offence; the nature, and severity, of the harm that might be suffered by individuals, among others.

ii) **Children's risk assessment**, includes an analysis on: the user base including the number of users who are children in different age groups; the level of risk children might encounter, considering type of priority content and non-designated content, features, functionalities or behaviors —including those enabled or created by the design or operation of the service—, and algorithms used by the service and how easily, quickly and widely content may be disseminated by means of the service; the level of risk of functionalities of the service might facilitate the presence or dissemination of content that is harmful to children, and how the design and operation of the service (including the business model, governance, use of proactive technology, measures to promote users' media literacy and safe use of the service, and other systems and processes) may reduce or increase the risks identified.

iii) **Adult user empowerment assessment (relevant content[256])**, includes an analysis on: the user base; the incidence of relevant content on the service; the likelihood of adult users of the service encountering relevant content —algorithms used by the service, and how easily, quickly and widely content may be disseminated by means of the service—; the likelihood of adult users with a certain characteristic or who are members of a certain group encountering relevant content which particularly affects them; the likelihood of functionalities of the service facilitating the presence or dissemination of relevant content, identifying and assessing those functionalities more likely to do so; how the design and operation of the service (including the business model, governance, use of proactive technology, measures to strengthen adult users' control over their interaction with user-generated content, and other systems and processes) may reduce or increase the likelihood of adult users encountering relevant content.

iv) **Content of democratic importance**: (i) News publisher content, whenever the internet service provider takes action[257] on this content, it should inform the publisher on: specificities of the action; reasons for that proposed action;

[256] For the purposes of the Bill, content is any which: encourages, promotes or provides instructions self-harm; if it incites hatred against people— (a) of a particular race, religion, sex or sexual orientation, (b) who have a disability, or (c) who have the characteristic of gender reassignment.

[257] According to the Bill, "taking action" in relation to content are to— (a) taking down content, (b) restricting users' access to content, or (c) adding warning labels to content, except warning labels normally encountered only by child users, and also include references to taking any other action in relation to content on the grounds that it is content of a kind which is the subject of a relevant term of service (but not otherwise).

explanation on how the provider took the importance of the free expression into account; a reasonable period within which the recognized news publisher may make representations. (ii) Protect journalistic content: duty to include provisions in the terms of service specifying: by what methods content present on the service is to be identified as journalistic content; how the importance of the free expression of journalistic content is to be taken into account when making decisions; the policies and processes for handling complaints in relation to content which is, or is considered to be, journalistic content.