EU Consumer Protection 2.0

Structural Asymmetries in Digital Consumer Markets, A joint report from research conducted under the EUCP2.0 project

Helberger, N.; Lynskey, O.; Micklitz, H.-W.; Rott, P.; Sax, M.; Strycharz, J.

Publication date
2021

Document Version
Final published version

License
Unspecified

BEUC The European Consumer Organisation

EU CONSUMER PROTECTION 2.0

Structural asymmetries in digital consumer markets

Natali Helberger
Orla Lynskey
Hans-W. Micklitz
Peter Rott
Marijn Sax
Joanna Strycharz

March 2021

ADESSIUM FOUNDATION
European University Institute — Robert Schuman Centre for Advanced Studies
IViR Instituut voor Informatierecht / Institute for Information Law
LSE Department of Law
Carl von Ossietzky Universität Oldenburg

EU Consumer Protection 2.0

Structural asymmetries in digital consumer markets

A joint report from research conducted under the EUCP2.0 project

Natali Helberger

Orla Lynskey

Hans-W. Micklitz

Peter Rott

Marijn Sax

Joanna Strycharz

Brussels, March 2021

Project information

The European Union Consumer Protection 2.0 (EUCP2.0) project is a research and advocacy initiative launched by BEUC with support from the Adessium Foundation, aimed at addressing the issues that plague the digital consumers of today and undermine the digital society as a whole. Particular focus is put on behavioural manipulation, exploitation of vulnerabilities, omnipresent personalisation affecting freedom of choice, as well as the rise of the largest digital platforms which have become an essential element in the modern society, yet without any responsibilities that would reflect this position.

This research will be used to formulate advocacy proposals and, following consultations with a variety of stakeholders, to power the forthcoming advocacy campaign. The primary aim is to advocate for changes to EU consumer law that would allow it to rise to the challenge of protecting the agency of modern-day digital consumers and, in consequence, their autonomy as citizens in a digital society.

The following three research areas were identified on the basis of BEUC's mapping input:

Area I. Surveillance, consent and the vulnerable consumer. Regaining citizen agency in the information economy.

As the framing study under the project, its primary aim was to offer a fitness assessment of the fairness paradigm enshrined in the Unfair Commercial Practices Directive in the context of behavioural monitoring, data mining and nudging practices of surveillance capitalism. Departing from an evaluation of the shortcomings of the average / vulnerable / targeted consumer conceptual framework in light of the profiling and behavioural influence practices of online businesses, the study moves to discuss the feasibility of the information and consent paradigm of the GDPR in addressing real-world management of access to personal data and the capacity of the data subject to give valid informed consent. The study offers an overall assessment of the structural asymmetries in today's digital consumer markets and proposes a new conceptual and regulatory approach to restore consumer agency and protect autonomous choice in the age of big data.

Area II. Personalised pricing and individualized marketing under EU consumer law: fairness and discrimination

Building upon the findings of the framing study, this research is centred on a consumer law analysis of market phenomena which arise in consequence of digital platforms holding personalized information on every user: personalized pricing and individualized marketing. Individualizing both price information and marketing message puts traders in control in what each individual consumer is allowed to know; thus placing them in the factual position of ownership of the information economy. Despite existing arguments of increasing economic efficiency, the near unanimous rejection of such practices by consumers, also those who could potentially stand to profit from them, adds fuel to the debate on fairness, trust and the societal and individual justice implications of traders being in control of the product and price information delivered individually to each user – and on the appropriate response that should be expected from data protection and consumer laws.

Area III. Online platforms, special responsibilities and the universal service regime

'From a consumer perspective, do online platforms provide services that should be considered essential'? The unique position of the largest digital platforms as necessary intermediaries (gatekeepers) in modern societies has laid the ground for asking questions about the essential nature of the services they provide, the existing parallels to the conceptual and regulatory framework for services of general interest (SGI) and the implications of adopting such a perspective. The study looks at how the special obligations previously associated with the classification could be applied to such 'gatekeeper' platforms, how their application could help protect societal values and mitigate the asymmetries of the digital market.

Contents

Part I

Surveillance, consent and the vulnerable consumer. Regaining citizen agency in the information economy

Natali Helberger[1], Hans-W. Micklitz[2], Marijn Sax[3] and Joanna Strycharz[4]

(in alphabetical order)

---

1 Distinguished University Professor of Law and Digital Technology, with a special focus on AI at the University of Amsterdam.

2 Professor for Economic Law, Robert Schuman Centre for Advanced Studies at the European University Institute and Finland Distinguished Professor, University of Helsinki, with a broad track record in European Private and Economic Law, National and European Consumer Law, Legal Theory.

3 Postdoctoral Researcher at the Institute for Information Law at the University of Amsterdam.

4 Assistant Professor and Postdoctoral Researcher, University of Amsterdam, ASCoR, with a focus on persuasive communication.

Part I: Table of Contents

Foreword

(1) The goal of this study is to critically assess the fairness paradigm enshrined in the Unfair Commercial Practices Directive (UCPD)[1] in light of the proliferation of data-driven commercial marketing strategies. In this context, we will revisit some key concepts of the Directive, including the *vulnerable consumer* and *aggressive practices*. Moreover, the study will explore ways towards fruitful interaction between consumer law and data protection law (GDPR) to help consumers effectively manage their data and improve their legal standing vis-à-vis advertisers. In so doing, legal analysis will be informed by insights from communication science and philosophy, and conducted by an interdisciplinary team (law, philosophy, and communication science).

(2) In the contemporary digital economy, platform and service providers offer their users digital environments that are optimized for searching, identifying, and targeting users' exploitable vulnerabilities. Put differently, in the digital economy consumers are constantly part of ongoing experiments aimed at finding out how and under what conditions they are manipulable. Most of the gears of this machinery for identifying and targeting vulnerability are invisible to consumers.

(3) To properly *protect* users against unfair commercial practices in the digital economy, we need a better understanding of how and under what conditions digital targeting practices render consumers vulnerable to persuasion and unfair forms of commercial communication. The current framework of the Unfair Commercial Practice Directive juxtaposes 'the vulnerable consumer' and 'the non-vulnerable consumer,' as if consumers neatly fall into either of those categories. However, as empirical findings demonstrate and conceptual approaches emphasize, vulnerability is not a stable *property* of a person. Not only do the *sources* of vulnerability differ – vulnerabilities that are inherent to the human condition and vulnerabilities that are situational in nature – but there are also different *states* of vulnerability. Therefore, in **Chapter 1** of the study we conceptualize Digital Vulnerability. This conceptualization also informs the analysis in Chapters 2 and 3.

(4) In **Chapter 2**, we investigate issues of consent and post-consent data management. To ensure consumers are provided with information needed to give consent, the GDPR places high requirements on data controllers and processors to inform consumers. More specifically, controllers are required to provide consumers with technical information regarding data collection and information about their rights. In consumer research, such

[1] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') OJ L 149, 11.6.2005, p. 22–39.

information has been portrayed as two dimensions of digital literacy related to privacy protection behaviours.[2] When more literate, consumers are expected to be empowered to take informed decisions and give or withhold their consent to data collection and processing. However, recent research puts these assumptions into question. First, in the context of online risks, Brandimarte, Acquisti and Loewenstein[3] have concluded a so-called *control paradox*. This assumes that control over sharing private information decreases one's privacy concerns and increases willingness to publish sensitive information. A similar effect of a *false feeling of security* has been concluded in relation to privacy seals[4] and targeting opt-out functionalities.[5] Findings like these further shed a critical light on the current law's strong reliance on consent as one of the most influential legal grounds for data processing in e-commerce settings, as well as the need to investigate effective post-consent data management entitlements.

(5) Based on insights from the previous chapters, **Chapter 3** offers a legal analysis of digital vulnerability, or rather, as this chapter frames it, digital asymmetries under European consumer law, and the UCPD in particular. Thereby Chapter 3 sets a counterweight to the proliferating debate on the use and usefulness of antitrust law to solve digital asymmetry through competition. But the UCPD will only turn into a powerful instrument if its basics are rethought. The clause on misleading practices focuses heavily on the 'information component' of commercial practices. However, if we take empirical findings on cognitive biases and tactics that tap into such biases seriously (see for example Waldman, 2019), it is evident that the provision (or omission) and presentation of information is but one aspect of the manipulative potential of contemporary digital choice architectures. The larger and more important question pertains to the structural *power relations* that are introduced by contemporary digital choice architectures. With their ability to constantly run experiments to identify and target any type of vulnerability that (some) users may experience – either because the vulnerability is already present or because it can be evoked/triggered – service and platform providers have attained a great position of power (Sax et. al, 2018). The structural power dynamics and the structural digital asymmetries introduced by the digital economy should serve as a starting point for rethinking European law on unfair commercial practices. The Chapter argues in favour of a reversal of the burden of proof that would render enforcement of the UCPD feasible (Willis 2020) and then evaluates whether structural digital asymmetry could be regarded as an aggressive practice, or as an infringement of professional

2 (Park 2013)

3 (Brandimarte, Acquisti, and Loewenstein 2013)

4 (Noort, Kerkhof, and Fennis 2008)

5 (Strycharz et al. 2019)

diligence. The Chapter concludes with some key take-aways for a possible reform of the UCPD.

(6) This report is the result of combined perspectives from law (Prof. Dr. Hans Micklitz, Robert Schuman Centre for Advanced Studies, European University Institute Florence; Prof. Dr. Natali Helberger, Institute for Information Law (IViR), University of Amsterdam), ethics (Marijn Sax, Institute for Information Law (IViR) and communication science (Dr. Joanna Strycharz, Amsterdam School of Communication (ASCoR), University of Amsterdam. The research for this report was concluded on 15 December 2020.

Chapter I. Digital vulnerability

1. Introduction

(7) In this Chapter, we will revisit the notion of consumer vulnerability. The idea(l) of the 'average consumer'[6] permeates large parts of European consumer law and has been pivotal in building a narrative of consumer empowerment and enabling consumers to protect themselves through active and well-informed choices in the marketplace. This is contrasted by the 'vulnerable consumer' – a concept that singles out certain groups of consumers that are more susceptible to unfair commercial practices than others, and less able to protect themselves. We will argue that, in digital markets, consumer vulnerability is not simply a vantage point from which to assess some consumers' lack of ability to activate their awareness of persuasion. In digital marketplaces, most if not all consumers are potentially vulnerable. Instead of singling out certain groups of consumers, digital vulnerability describes a universal state of defencelessness and susceptibility to (the exploitation of) power imbalances that are the result of increasing automation of commerce, datafied consumer-seller relations and the very architecture of digital marketplaces. Finally, we will demonstrate why using digital technology to render consumers vulnerable is the epitome of an unfair digital commercial practice.

(8) With the digitization of consumer markets, consumers as well as traders increasingly rely on algorithmic profiling, automated decision-making, and predictive analytics. Nothing has made that more obvious than the Covid-19 crisis, with large parts of consumer activity moving into online space and onto digital platforms such as Amazon, Bol.com, eBay, and online supermarket ordering systems. These systems are largely data-driven, using data to recommend services, remind us of products that we might still like to buy, or provide us with personalized offers and promotions. Our online consumer behaviour is registered 24/7,

---

6 In the sense of a consumer who can be considered to be reasonably well informed, observant and circumspect, European Court of Justice, Case C-210/96 *Gut Springenheide and Tusky* [1998] ECR I-4657, para 31.

monitoring every step in the consumer journey, submitting us to a constant stream of A/B testing and interventions to optimize the system and the consumer-seller relationship. Data-driven commercial strategies are embedded in a sophisticated web of smart speakers, intelligent household appliances, in-store surveillance, apps and trackers that feed into the stream of data – data that will ultimately create virtual representations of consumers, and, perhaps more importantly: consumer 'commercialisation potential'. The overall objective of these practices is to render consumers receptive to digital marketing strategies that use digital technologies to optimize commercial practices with the goal of selling products and services to consumers. Doing so can enhance the consumer experience, help the consumer to find the goods and services they are looking for and intensify and personalize the relationship between trader and consumer. The use of digital technology and data analytics, however, can also be the source of new power imbalances between consumers and traders, and new forms of unfair commercial practices.

(9) The creation of personalized 'persuasion profiles'[7] in combination with the (ability to implement) adaptive targeting strategies that would deliver the right message at the right time and place to the right consumer lies at the heart of new targeted advertising strategies that seem increasingly to form the backbone of online advertising.[8] These strategies can range from contextual advertising and advertising strategies that are based on rather broadly defined demographics, such as age or gender, to more fine grained targeting (for instance: matching demographic characteristics with observed behaviour) to very fine-grained forms of psychographic targeting that rely on psychological insights into the personality and behaviour of a consumer, her values, opinions and interests.[9] Persuasion profiles are only the tip of the iceberg. Dark patterns are architectural 'user interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions'.[10] Practices can range from default settings, bait and switch, sneak into basket, disguised advertising interfaces, forced continuity or design choices that make price comparison more difficult.[11] In addition, digital price discrimination uses personal characteristics to differentiate prices and marketing conditions, thereby making consumers vulnerable to misleading claims about, for example, the price (if they are not aware that they are paying a higher price than other consumers), the availability of a product or service, or its conditions, but also more generally differential or even

---

7 Defined as "collections of estimates of the expected effects of different influence principles for a specific individual. Hence, an individual's persuasion profile indicates which influence principles are expected to be most effective." (Kaptein et al. 2015b, 41)

8 (Strycharz et al. 2019)

9 (Burkell & Regan, 2019)

10 (Chivukula et al. 2019; Mathur et al. 2019; Frobrukerradet 2018)

11 (Mathur et al. 2019; Cara 2019)

discriminatory marketing practices. Technology is used to shape the very relationship between advertisers, sellers and consumers and give it permanence and knowledge of the consumer that evolves over time, and intensifies with time.[12] Examples include e-commerce, media or fitness apps that users install on their mobile devices, but also the proliferation of chatbots and virtual assistants whose very mission is to adapt to their users by learning about them and generating knowledge and the power to persuade, but also to proactively engage in triggering – or even creating – (new) vulnerabilities.[13]

(10) Unfair commercial practice law can have an important role in assessing the fairness of these practices.[14] Indeed, the law's capacity to do so will be an important focal point of this report. A central element in assessing the fairness of any commercial practice is the underlying concept of the consumer, and the extent to which they can be expected to deal in a reasonably well-informed, observant and circumspect way with these practices, or whether they belong to the category of so-called vulnerable consumers. Originally designed to single out situations in which consumers, for reasons largely related to their own personal characteristics (for example their age), are particularly susceptible to forms of market persuasion, the concepts of average and vulnerable consumers play an important role in assessing the fairness of a commercial practice. The question that this Chapter discusses is: what protection can the concept of consumer vulnerability offer the digital consumer, is the distinction between the average and the digital consumer still fit for the digital age, and if not, do we need a new understanding of 'digital vulnerability' and what would its elements be?

2. The concept of consumer vulnerability under current consumer law: a closer look

(11) The concept of vulnerable users plays an important role in law generally, not only in consumer law. The vulnerability concept is often used to identify users, or groups of users, that require particular regulatory/policy attention because of their lack of bargaining power, structural inequalities and other market or social conditions that make them more susceptible to harm (for example in the form of discrimination or unequal treatment). At times, it is also used as a concept to allow differentiation in situations in which uniform treatment of all would lead to unfairness for some.[15] For example, Peroni and Timmers show how in the case law of the European Court of Human Rights, the acknowledgement of vulnerability status for particular groups (such as Roma, people with mental disabilities,

12 (Bol et al. 2018)

13 (Calo 2013, 999)

14 (Micklitz and Namyslowska 2020a; Natali Helberger 2016)

15 (Leczykiewicz and Weatherill 2016)

people living with HIV, and asylum seekers) has led the court to find special positive obligations on the part of the state, increase the weight of harm in proportionality analysis, and reduce states' margin of appreciation.[16] Malgieri and Niklas[17] trace the development of vulnerability as a concept in data protection law, mostly confined to the case of minors who are less aware of potential risks and consequences of data protection and who therefore warrant a higher level of protection (for example with respect to the right to transparency, profiling, and informed consent).[18] However, in contrast to human rights law and data protection law, vulnerability has received an explicit legal definition in Article 5 3) Unfair Commercial Practices Directive.[19]

a) Vulnerability in current consumer law

(12) Article 5 (3) UCPD describes the vulnerable consumer as a member of a 'clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee.' As such, the concept of the vulnerable consumer cannot be seen separately from the concept of the average consumer. Together, the concepts of average and vulnerable consumer form the vantage point from which a commercial practice must be assessed (Waddington, 2013). The way both concepts interact showcases an inherent tension in consumer law between protecting users as the weaker party in commercial dealings and enabling consumers to play their role as active and autonomous market participants.

(13) As a rule, commercial practices must be assessed from the perspective of the average consumer, the prototype of European consumer law, who is 'reasonably well-informed and reasonably observant and circumspect' (Recital 18 UCPD). It is the perspective of the average consumer that is in the first place relevant when assessing the fairness of a particular practice. Article 5 (3) describes the exception to the rule [20] A small range of practices, namely practices that are 'likely to materially distort the economic behaviour only of a clearly identifiable group of consumers who are particularly vulnerable to the practice' (Article 5 (3) UCPD), if specifically targeted at such consumers are to be assessed from the perspective of an 'average member' of a group of vulnerable consumers. A practice that might be

16 (Audrey R Chapman and Benjamin Carbonetti 2011; Peroni and Timmer 2013)

17 (Malgieri and Niklas 2020)

18 Recitals 38, 58, 65 and 75 GDPR.

19 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA relevance)

20 (Micklitz and Namyslowska 2020a) See (Peroni and Timmer 2013), 1061, showing that a similar dichotomy characterises the dominant stance in the treatment of vulnerability in human rights law

acceptable from the perspective of the average consumer may constitute unfairness when targeted at, and assessed from, the perspective of the vulnerable consumer.

(14) Consumers, at least under the UCPD, can be considered vulnerable because of their personal characteristics, namely mental or physical infirmity, age or credulity and the effect that these characteristics have on their ability to deal with commercial practices. There is some discussion in the literature as to what extent this list is exhaustive or not.[21] Common to all the categories listed in Article 5(3) UCPD is the focus on internal characteristics within the consumer that affect their ability to adequately deal with commercial practices. Not part of the analysis are external factors such as the degree of exposure to certain practices, or the consequences that such practices may have for an individual consumer.[22]

(15) Unlike in human rights law or data protection law, where qualification as a vulnerable group can trigger particular legal obligations or protective duties for states or stakeholders, targeting messages at vulnerable consumers is not in itself an unfair practice, nor does it directly translate into extra (fiduciary or protective) responsibilities or additional information obligations for sellers. Nor, too, is targeting commercial messages at vulnerable consumers an unfair commercial practice as such (Annex 1 UCPD, apart from No. 28 – targeting commercial practices directly at children). Consumer vulnerability can be a factor when assessing whether a practice qualifies as either misleading or aggressive. The judge will then assess that practice from the perspective of that particular group.[23] Bluntly speaking, the current role of the vulnerable consumer criterion is that of a vantage point from which commercial practices can be assessed, nothing more, and nothing less.

b) Rethinking vulnerability – theoretical considerations

(16) For a critical discussion of the current concept of consumer vulnerability in the context of digital market practices, and before moving to a discussion of digital vulnerability in section 3, it is useful to position Article 5 (3) UCPD in the context of the broader theoretical vulnerability discourse. This is so for at least two reasons: first, it helps us to understand (the limitations of) the current way in which the UCPD defines consumer vulnerability. Second, it informs our understanding of the future role that unfair commercial practice law should play in dealing with digital consumer vulnerability.

(17) Conceptualizing consumer vulnerability under the UCPD (also the GDPR and human rights law) has traditionally been an attempt to identify particular groups of consumers, or characteristics in consumers, that render a consumer or a group of consumers (such as

---

21 (Micklitz and Namyslowska 2020a; Howells, Twigg-Flesner, and Wilhelmsson 2018; Duivenvoorde 2013)

22 (Duivenvoorde 2013)

23 Reich, 2016, points out that there are, for example, no specific information obligations in the directive, p. 153. Doubtful at least whether the vulnerability criterion plays a role in the context of Arts 6-8, Howells, 2018, 70.

minors, or the elderly) more susceptible to harm, unequal treatment and unfairness.[24] This is what Cole calls the 'victim approach'[25] to vulnerability, as the concept is used to draw attention to the inherent weakness of particular groups, or their inability to fend for their own interests. This framing of consumer vulnerability as a diminished capacity to understand advertising, or to maximise utility and wellbeing,[26] resonates with conceptualisations of consumer vulnerability in the market research and behavioural literature.[27] It also corresponds rather well with European liberal ideals about the role of consumers as active market participants who through their informed choices help to create the conditions of fair and functioning marketplaces.[28] The vulnerable consumer with their inherent and external limitations is an exception to that ideal.

(18) More recent critical advances in the vulnerability literature have criticized this approach of identifying particular groups of vulnerable users as unnecessarily stigmatizing, patronising and disconnected from social reality.[29] Among the most prominent and influential proponents of an alternative approach to vulnerability is Martha Fineman with her vulnerability theory. According to Fineman, vulnerability is a consequence of human embodiment, carrying with it 'the ever-present possibility of harm, injury, and misfortune' [30] and therefore 'no individual can avoid vulnerability'. According to this universal understanding of vulnerability, vulnerable consumers are not the exception; they are the rule. This is essentially the opposite approach to that stipulated by the UCPD.

(19) Concerns about the unnecessarily static and stigmatising effects of a non-universal approach to consumer vulnerability also resonate in the critical consumer law literature. Here, legal scholars have criticized the rigidity of the distinction between either the average or the vulnerable consumer, and the risk of framing consumer protection law as something that only 'the weak' are in need of.[31] Arguably, the digitisation of consumer markets is further fuelling these concerns. As Calo points out, digital marketing strategies 'tend [] to collapse the ethical and legal distinction between the ordinary and vulnerable consumer'.[32] In other words: the vulnerable consumer is no longer the exception, nor is the ordinary or average

---

24 (Duivenvoorde, B.B. and CSECL (FdR) 2015)

25 (Cole 2016)

26 (Craig-Smith and Cooper-Martin 1997)

27 (Baker, Gentry, and Rittenburg 2005)

28 European Economic and Social Committee, EU Consumer Policy strategy 2007- 2013 Empowering Consumers, Enhancing Their Welfare, Effectively Protecting Them, at 2-6, COM (2007) 99 final (Mar. 13, 2007) [hereinafter Empowering Consumers].

29 (Malgieri and Niklas 2020; Cole 2016)

30 (Albertson Fineman 2008)

31 (Howells, Twigg-Flesner, and Wilhelmsson 2018, 28–29)

32 (Calo 2013, 1033)

consumer the rule. Every consumer has a persuasion profile.[33] The digitization of consumer markets and electronic transactions has enabled entirely new forms of personalized persuasion strategies that discover, and build on, individual biases, weaknesses, preferences and needs and that can be directed, very purposefully, at *making consumers – even those that do not belong to the typical categories of vulnerable consumers – vulnerable, in the sense of affecting their ability to rationally deal with a particular marketing practice.*

(20) Interestingly, in more recent policy documents from the European Commission, a subtle shift towards this more universal thinking about vulnerability can be observed and a push for abandoning the static, categorical definition can be discerned.[34] A more recent interpretation of consumer vulnerability offered by the European Commission recommends taking 'into account that consumer vulnerability is situational, meaning that a consumer can be vulnerable in one situation but not in others, and that some consumers may be more vulnerable than others.'[35]

(21) For some, this more universal understanding of consumer vulnerability probably goes too far. Reich, for example, suggests that the concept of consumer vulnerability needs to be distinguished from the concept of consumer weakness in order to avoid expanding the concept too far.[36] Concerns about lack of distinctiveness and ability to take into account individual conditions also resonate in the writings of some critiques of universal vulnerability theory. It is true that Fineman and others concede:

> [b]ecause we are positioned differently within a w/eb of economic and institutional relationships, our vulnerabilities range in magnitude and potential at the individual level. Undeniably universal, human vulnerability is also particular: it is experienced uniquely by each of us and this experience is greatly influenced by the quality and quantity of resources we possess or can command (p. 9).

(22) Still, the universal approach has been criticized because it would leave too little room for considering individual differences, for example because of identity or social status. It can thereby precisely enforce the binary distinction between vulnerable/non-vulnerable that vulnerability theory sought to abolish, but in reverse.[37]

(23) Critics of Fineman's vulnerability theory have therefore argued in favour of further building on vulnerability theory in a way that acknowledges the way identities and privileges

---

33 In this sense also Micklitz & Nanyslowska, UGP-RL Art. 5 RN 64, who point to the limited usability of the fictive notion of the average consumer in the light of algorithmic personalization strategies

34 London Economics, Consumer vulnerability across key markets in the European Union, Brussels, 2016 https://ec.europa.eu/info/sites/info/files/consumers-approved-report_en.pdf

35 European Commission, Understanding Consumer Vulnerability in the EU's key markets, Brussels, 2016, https://ec.europa.eu/info/sites/info/files/consumer-vulnerability-factsheet_en.pdf

36 (Reich 2016, 141)

37 (Cooper 2015; Cole 2016)

influence social practices.[38] After all, not all people are alike, some are more affluent, privileged or better equipped than others. To account for the inequalities this may create, it is necessary to acknowledge the influence of different identities and privileges within each of us as consumers and how they influence social practices.[39] In a similar vein, Cole criticizes the fact that universalism makes it impossible to acknowledge distinctions between particularly vulnerable users: ' The concept has been rendered so broad as to obscure the needs of specific groups and individuals, undermining its promise as a conceptual frame to understand and challenge systemic inequalities'.[40] In response, critics have suggested moving beyond using vulnerability as a label, and transferring attention towards the factors that transform the theoretical possibility of being vulnerable (see section 3, dispositional vulnerability) into a concrete situation of unfairness.[41]

(24) When looking into potential sources of vulnerability, or factors that contribute to making consumers vulnerable, we can turn to a rich body of research in behavioural economics and psychology. Researchers in that field have for some time now acknowledged that categorical approaches, such as the one stipulated in Article 5 (3) UCPD), essentially disregard external and societal factors that contribute to making consumers vulnerable.[42] It also falsely creates a perception that consumers are either vulnerable or not. As Baker et al. point out, 'actual vulnerability arises from the interaction of individual states, individual characteristics, and external conditions within a context where consumption goals may be hindered and the experience affects personal and social perceptions of self'.[43] In consumer research, the term vulnerability has a broad range of applications, such as individual characteristics (for instance, age, race, physical capabilities), social phenomena (such as stereotyping), business practices (for example, store layouts, marketer manipulations), and environmental forces (such as natural disasters).[44] In general, the consumer research literature relates to two main streams of thought: vulnerability as a result of disadvantages and of marketer manipulation. Regarding disadvantages, research in this stream focuses on individuals disadvantaged through their individual characteristics, socioeconomic status and available resources.[45] In the case of manipulation, researchers have, for example, examined why and how

38 (Cooper 2015)

39 (Cooper 2015)

40 (Cole 2016, 267)

41 (Peroni and Timmer 2013, 1074), see also Luna, suggesting a layered concept with a focus on the aspects that contribute to vulnerability at its source

42 (Baker, Gentry, and Rittenburg 2005)

43 (Baker, Gentry, and Rittenburg 2005, 134)

44 (Baker, Gentry, and Rittenburg 2005)

45 (Hill and Sharma 2020)

interpersonal influence can make consumers vulnerable to marketing scams.[46] Others point out that it is not so much belonging to a group of particular consumers that marks these individuals as vulnerable, but 'it is the circumstances that consumers face that determine their vulnerability'.[47] In a similar vein, Cartwright suggests also including contextual, relational and situational factors, and draws a useful distinction between informational vulnerability (the one that the UCPD also focuses on) and pressure, supply, redress and impact vulnerability.[48] Finally, Berg[49] underlines that, when studying vulnerabilities, one needs to draw a clear distinction between vulnerabilities and capabilities. While past research has often treated both these constructs as synonymous, reduced capabilities should be seen as possible individual, internal vulnerability drivers, and they should be distinguished from external vulnerability drivers composed of markets' varying consumer conditions or the digital choice architecture, and that are not related to the capabilities of a single individual. The findings from the behavioural literature hence confirm the intuitions of critical theoretical vulnerability thinkers that indeed everyone may experience vulnerability in some situations, and that consumers may vary in the extent to which they are vulnerable in different contexts—across time and place.[50]

(25) Looking forward, then, an important contribution of recent theoretical advances in the thinking on vulnerability theory is the recognition that vulnerability is not a state of exception, reserved for particular groups of consumers, but a universal condition. This is also true of digital markets. An important aim behind digital market practices is to identify those differences and individual trigger points. Thereby consumer vulnerability becomes a design goal that systems can be optimized for. The behavioural literature has helped to advance our insights into the factors that can contribute to vulnerability, pointing to an array of internal, contextual, relational, and situational factors.

(26) Moreover, both the theoretical and empirical literature shows that vulnerability is not only caused by internal factors (as stipulated in Article 5 (3) UCPD). Instead, equally or even more influential are external factors and broader societal or institutional arrangements that 'originate, sustain, and reinforce vulnerabilities'.[51] Proponents of a more universal theory of vulnerability argue that it is not (inherent) vulnerability that distinguishes users and creates inequalities, but rather 'systems of power and privilege that interact to produce webs of

46 (Langenderfer and Shimp 2001)

47 (Hill and Sharma 2020, 4)

48 (Cartwright 2015)

49 (Berg 2015)

50 (Hill and Sharma 2020)

51 (Peroni and Timmer 2013, 1059)

advantages and disadvantages'.[52] In other words, next to individual factors it is necessary to explore the external and systemic factors that contribute to consumer vulnerability, which is what section 1 (3) c) will do for the case of digital consumer vulnerability.

(27) Finally, the fact that vulnerability is not (only) an inherent condition but the product of external market or societal circumstances and power structures contains important policy implications. Essentially this means that consumers are not simply vulnerable, but that some market structures and configurations make them vulnerable, or even worse: exploit their vulnerabilities. This insight can have important implications for consumer law and policy. Whereas current unfair commercial practice law is essentially focused on accommodating internal vulnerabilities, a more universal vulnerability perspective that also takes into account external factors shifts the analytical focus from vulnerability as a benchmark or vantage point towards an investigation of the role that unfair commercial practice law can have in addressing these more systemic and external circumstances and potential power imbalances. Indeed, as Fineman has argued, vulnerability theory can be a 'powerful conceptual tool with the potential to define an obligation for the state to ensure a richer and more robust guarantee of equality than is currently afforded under the equal protection model' (9). In practice this means that to truly understand and conceptualise consumer vulnerability it is necessary to explore market practices, systemic and institutional conditions that create vulnerability in the first place. This is what the following section will do for the case of digital market practices.

3. Towards a concept of digital vulnerability

(28) In response to mounting criticism of the traditional interpretation of the vulnerable consumer, the static, categorical definition seems to have been abandoned in more recent guidance documents.[53] In a more recent communication, the European Commission defined the vulnerable consumer as:

> A consumer, who, as a result of socio-demographic characteristics, behavioural characteristics, personal situation, or market environment:
>
> • Is at higher risk of experiencing negative outcomes in the market;
>
> • Has limited ability to maximise his/her well-being;
>
> • Has difficulty in obtaining or assimilating information;
>
> • Is less able to buy, choose or access suitable products; or

[52] (Albertson Fineman 2008, 16)

[53] London Economics, Consumer vulnerability across key markets in the European Union, Brussels, 2016 https://ec.europa.eu/info/sites/info/files/consumers-approved-report_en.pdf

- Is more susceptible to certain marketing practices.[54]

(29) It is worth noting that this new definition by the Commission has moved away from the original focus of Article 5 (3) UCPD on internal factors and group vulnerability, towards taking into account not only a more universal conception of vulnerability, but also the relevance of external and situational factors, such as the market environment (see previous section). But what does this mean for digital vulnerability in concrete terms?

(30) With digital practices, commercial messages are only one part in a larger, systemic approach to influencing consumer behaviour. The message is part of the system and can no longer be separated from the technical infrastructure that generates it, because it is a result of what Kaptein *et al.*[55] call an 'adaptive persuasive system'. Accordingly, to be able to evaluate commercial practices in terms of their fairness, it is not enough to evaluate the message; the systemic set-up and the way technology shapes the relationship between consumer and advertiser should also figure prominently in such an analysis.

(31) It follows that a concept of digital vulnerability fit for the digital society should somehow mirror the industry's relentless search for experimental and creative digital marketing practices that seek to 'optimize' consumers' patterns of behaviour. The industry tries to identify and target different sources and triggers of vulnerability, as well as a wide range of circumstances under which consumers are – or can be rendered – vulnerable. Our concept of vulnerability should be similarly *dynamic*.

a) Conceptual refinements needed

(32) Before one starts thinking about the conceptual *refinements* that are needed to arrive at a notion of digital vulnerability, it helps to ground such an analysis in a basic, uncontroversial understanding of what the concept of vulnerability generally is about. Anderson[56] provides a helpful minimal definition of vulnerability: 'a person is *vulnerable* to the extent to which she is not in a position to prevent occurrences that would undermine what she takes to be important to her.' Thus vulnerability is about one's relation to the world, the forces (social, physical, technical) in the world that can affect anything one deems important, and one's (lack of) control or power over those forces. In the context of digital consumer markets, then, vulnerability is about the power or ability of commercial actors to affect the decisions, desires, and behaviour of the consumer in ways that the consumer, all things considered, does not condone, but also is not in a position to prevent. The challenge, then, is to refine the concept of vulnerability in such a manner that it allows us to capture *all* those ways in

---

54 European Commission, Understanding Consumer Vulnerability in the EU's key markets, Brussels, 2016, https://ec.europa.eu/info/sites/info/files/consumer-vulnerability-factsheet_en.pdf

55 (Kaptein et al. 2015)

56 (Anderson 2014, 239)

which consumers can be affected adversely by actors in digital marketplaces without being able to prevent those occurrences. Moreover, vulnerability does not originate solely in a person's (fixed) characteristics, but in a person's *relation* to other actors.

(33) A first, foundational, conceptual refinement can be found in the work of Rogers, Mackenzie, and Dodds (2012) and Mackenzie, Rogers, and Dodds (2014). Their taxonomy of vulnerability differentiates between *sources* and *states* of vulnerability. This basic distinction will help structure the following discussion.

i. Sources of vulnerability

(34) To start with sources of vulnerability, one can distinguish between inherent and situational sources. Inherent vulnerabilities are 'intrinsic to the human condition' and 'arise from our corporeality, our neediness, our dependence on others, and our affective and social natures'.[57] These are the kinds of vulnerabilities Fineman[58] discusses. For example, all human beings need social and affective relations and are vulnerable to those relations falling away due to circumstances beyond their own control. Another example is people's need for a healthy body and mind to live a flourishing life, and the associated inherent vulnerability to diminishing health due to a wide range of factors. In contrast, situational vulnerabilities are those vulnerabilities that are not an intrinsic part of the human condition, but only arise in particular contexts or situations. A variety of influences of a different nature – 'personal, social, political, or environmental' – can cause or exacerbate vulnerabilities. For example, a failed relationship can make one vulnerable to having one's feelings hurt, a storm can make one vulnerable to having one's property destroyed, and collection of large amounts of data can make one vulnerable to having one's persuasion profile inferred and used for targeting practices.

(35) It is important to emphasize that different people live, act, and decide under different circumstances. So the influence of potential sources of vulnerability on the *specific* situation of an individual is *mediated* by the *specific* circumstances of that person. People live under different socio-economic conditions, which co-determine their ability to respond to diverse sources of vulnerability. Moreover, every person has (to some degree) different psychological characteristics which determine 1) one's susceptibility to particular influences, as well as 2) one's ability to *react* to those influences.

(36) Another important element to consider is the temporal dimension of situational vulnerabilities. Inherent vulnerabilities are intrinsic to the human condition and are therefore, in principle, always present. But situational vulnerabilities can 'be short term,

---

57 (Mackenzie, Rogers, and Dodds 2014, 7)

58 (Albertson Fineman 2008)

intermittent, or enduring'.[59] For example, a person can experience an unpleasant incident at work and, as a result of that incident, be susceptible to negative or harmful social influences for a few days due to feeling very hurt or insecure. We can, however, also think of situational vulnerabilities that are rather persistent, without being inherent vulnerabilities. Think of a person that suffers from a non-chronic disease for months or years. Their health status may make them situationally vulnerable to being adversely affected by particular influences for longer periods of time (months or years).

ii. States of vulnerability

(37) Besides asking what causes vulnerabilities, we should also ask *how* vulnerabilities can manifest themselves. This is where the different *states* of vulnerability come in: vulnerabilities can be 'dispositional' and 'occurrent'.[60] (Both inherent and situational vulnerabilities can be dispositional and occurrent). The category of 'dispositional vulnerabilities' roughly translates to *potential* vulnerabilities. Put differently, dispositional vulnerabilities are those vulnerabilities that have not yet manifested themselves but that could do so given the underlying circumstances – and here one can think of all the inherent and situational sources already discussed. The category of 'occurrent vulnerabilities' simply refers to those dispositional vulnerabilities that also actually manifest themselves. Mackenzie, Rogers, and Dodds[61] provide a helpful example to explain this admittedly abstract but important distinction:

> [A]ll fertile women of childbearing age are dispositionally vulnerable to life-threatening complications in childbirth. But whether or not a pregnant women is occurrently vulnerable to such complications will depend on a range of factors, both inherent and situational, such as her physical health, medical history, socioeconomic status, geographical location, access to health care, and cultural norms relating to pregnancy and childbirth.

(38) One does not necessarily need to adopt these specific terms to see the usefulness of the distinction. To be able to see and, if needed, address all (potential) vulnerabilities, it is necessary to look beyond those vulnerabilities that already actually obtain *right now*. Because dispositional vulnerabilities may *seem* less immediate than occurrent vulnerabilities (which have, by definition, already materialized), it is easy to overlook their significance. In the digital society, however, dispositional vulnerabilities require as much attention as occurrent vulnerabilities. Many situations and contexts involve a structural yet latent potential for triggering or creating vulnerabilities that have not yet materialized. Think, for instance, of a digital service that collects large amounts of user data to infer persuasion profiles. The mere fact that the digital service holds persuasion profiles of its customers

---

59 (Mackenzie, Rogers, and Dodds 2014, 7)

60 (Mackenzie, Rogers, and Dodds 2014, 8–9)

61 (Mackenzie, Rogers, and Dodds 2014, 7)

renders those customers *dispositionally* vulnerable to, for instance, manipulation. Even if a company does not use those persuasion profiles *right now*, we can and should still ask whether collecting such persuasion profiles is desirable. Dispositional vulnerabilities warrant special attention in our contemporary digital marketplaces, where data-driven dynamically adjustable digital choice architectures can not only identify inherent (ever-present) vulnerabilities, but can also learn/infer how different consumers can be rendered vulnerable under different conditions.

b) Digital vulnerability is architectural

(39) Building on the basic distinction between sources and states of vulnerabilities, we now turn to specific characteristics of the digital marketplace that introduce the need for a concept of digital vulnerability. To fully understand vulnerabilities in the digital society, we propose that the *architectural* nature of vulnerabilities bears emphasis. An increasing number of interactions between consumers and sellers take place within digital choice architectures. To understand vulnerabilities in the digital society, we need to understand the *properties* of such digital choice architectures.

(40) The term 'choice architecture' was popularized by Thaler and Sunstein.[62] In their book *Nudge*, they explained how choice architectures can be designed to change behaviour, by anticipating known cognitive and affective biases in their design. They mainly focused on analogue choice architectures that are first designed and then put into place (semi)permanently. After the 'agile turn',[63] however, such (semi) linear design processes have been transformed. Contemporary digital choice architectures are 1) data-driven, 2) dynamically adjustable, and 3) personalizable. These properties allow for constant experimentation by and optimization of choice architectures.

(41) Because digital choice architectures are data-driven, they can collect user data *continuously*, allowing choice architects to learn how different users interact with the digital environment. The inferred behavioural patterns can be used to propose changes to the digital environment to change patterns of behaviour to secure (more) desirable outcomes for the vendor. This is where the significance of *dynamic adjustability* becomes clear. Contemporary digital choice architectures can be adjusted at any given time. Moreover, different 'versions' of a digital environment can be run at the same time (for example the by the now (in)famous A/B testing) to run experiments which allow one to test the effect of different design choices in real time. The insights from these experiments can then be used to personalize elements of the choice environment in order to optimize the behaviour patterns of groups of users or individual users. This entire process of collecting user data, running experiments, and making

62 (Thaler and Sunstein 2008)

63 (Hoboken and Gürses 2018)

adjustments is *cyclical* rather than *linear*. Due to this cyclical nature of contemporary digital commercial practices, a certain 'depth' also pertains to the resulting commercial relations and their potential for exploitation of vulnerabilities. By constantly learning more about one's consumers' characteristics and their responses to particular cues, the potential for effective manipulation also grows.[64]

(42) It is important to emphasize that operating one's choice architecture in this manner is relatively easy nowadays. Consider the app economy, with availability of affordable off-the-shelf services that help app developers to 'optimize' their apps roughly as described above. Both Apple and Google – which together dictate the terms of the app economy as intermediaries through their app stores – offer extensive support programs for app developers.[65] Google also offers app developers its Firebase[66] off-the-shelf mobile and web app service, with a wide range of built-in analytics and optimization services.

(43) In terms of consumer vulnerabilities, these contemporary digital choice architectures essentially offer an infrastructure to *automate* the *continuous* search for exploitable consumer vulnerabilities. 'Business analytics and optimization' practices are aimed at finding out how to get consumers to 'engage' with products and services, and how to 'convert' them as efficiently as possible. In practice, this comes down to continuously running experiments to discover *any* kind of psychological tendency or cognitive or affective bias that can be leveraged for growth. Here the importance of focusing on dispositional vulnerabilities becomes clear again. Contemporary businesses do not limit themselves to identifying and targeting clearly observable and already present vulnerabilities; quite to the contrary, the real competitive edge resides in the ability to identify and target personal circumstances and characteristics that make a person dispositionally vulnerable but that have not yet resulted in actual, occurrent vulnerabilities.

(44) In the digital society, vulnerability is architectural because the digital choice architectures we navigate daily are designed to infer or even create vulnerabilities. The vulnerabilities – be they dispositional or occurrent – that consumers can experience are not an unfortunate by-product of digital consumer markets; vulnerabilities are the product of digital consumer markets.

(45) To concretize these conceptual remarks on the architectural dimension to digital vulnerability, consider the following example. Platforms such as Facebook, Instagram, YouTube, Twitch, and TikTok have an interest in maximizing data flows between user and

---

64 (Susser, Roessler, and Nissenbaum 2019)

65 See, e.g., Google's 'Google Play Guides' and their 'Academy for App Success' (https://developer.android.com/distribute/best-practices) and Apple's extensive guides on 'Business & Analytics' (https://developer.apple.com/app-store/articles/).

66 https://firebase.google.com/

platform. Such platforms also control the digital choice architectures within which privacy policies are presented to users and users must consent to particular data practices. This complete control over the choice environment can, of course, be used to gently nudge users towards those consent options which maximize data flows. Digital vulnerability is at play here in (at least) two distinct ways. First, user data can be employed to 'optimize' the privacy settings environment for maximal data flows based on knowledge about how users interact with these choice environments. Second, and related, by 'optimizing' the privacy settings environment for maximal data flows, platforms can, in turn, further strengthen their position of power by gaining even more insight into the behaviour and psychology of their users. A telling example was recently provided by internal documents that were unsealed because of a lawsuit in the USA. In the unsealed document, internal communications between Google employees showed that even those that were involved with the design of the privacy settings often failed to understand how those settings worked.[67]

c) Digital vulnerability is relational

(46) So far, we have established the existence of different sources and states of vulnerability, and that contemporary digital choice architectures offer an infrastructure to identify and exploit a wide range of vulnerabilities by design. An additional perspective that requires elaboration is the *relational* nature of vulnerabilities in the digital society. People are not (just) vulnerable in total isolation; more often than not, it is precisely people's relational ties to others that make them vulnerable to other actors and influences.

(47) Consider, for example, the properties of digital choice architectures discussed above. The potential for identifying and targeting vulnerabilities grows as consumers keep using a particular service or app for a longer period of time. Usage over time means collection of user data over time, which translates to more insights into the vulnerabilities of the user, which in turn translates into more possibilities for efficacious adjustments of the choice architecture to influence behaviour over time. Unsurprisingly, commercial digital services often seek to build ongoing relationships with their users, by 'engaging' them and getting them 'hooked'.[68] Ongoing commercial relationships grow the potential for exploitation of vulnerabilities.

(48) Another important consideration is the often-asymmetrical nature of ongoing commercial relationships. As consumers keep using the same services, apps or platforms over time, the commercial entities offering those services, apps or platforms will be able to collect and analyse more user data and, as a result, be better able to identify exploitable vulnerabilities. Put simply: as commercial digital relations persist over time, power imbalances become

---

67 (Cox 2020)

68 (Eyal 2014)

more significant as a direct result of the ongoing relationship. This consideration aligns well with the consideration above about the 'depth' component of ongoing commercial relationships and the increasing potential for effective manipulation. Moreover, as consumers use a service, app or platform for longer periods of time, the more 'intense' the relationship may become. As consumers get accustomed to a particular service, app or platform, they may have a harder time exiting those services, apps or platforms, or switching over to other suppliers. So the better a seller is able to build an ongoing relationship with a user (partly as a result of the seller's increased knowledge about the user's persuasion profiles), the closer one gets to a situation that resembles (or even constitutes?) a situational monopoly.[69]

(49) Trust also plays an important role in the process of building ongoing relationships with users in datafied environments and the associated potential for exploiting vulnerabilities. Conceptually, trust and vulnerability are – necessarily – *intertwined*.[70] Trust always exists in the absence of certainty; trust under conditions of absolute certainty ceases to be trust. It follows that by trusting someone or something, one *necessarily* makes oneself dispositionally vulnerable to having that trust betrayed.[71] Now, to be sure, the intertwinement of trust and vulnerability is a fact of life and not bad as such. But trust can of course be *exploited* to render people vulnerable and, in turn, exploit these vulnerabilities. This is where contemporary digital choice architectures come in, for they are the types of environment that are especially suitable for exploiting trust to render consumers vulnerable.

(50) To see why, consider that 'trust is a psychological state that represents the trusted person or object as trustworthy, and this may or may not actually be the case'.[72] In other words, trust and trustworthiness can come apart:[73] 'Showing that people trust (within) a design does not imply that it is trustworthy, nor the other way around'.[74] Trust is a psychological state that can be evoked, instilled or engineered, whereas trustworthiness refers to the actual factual circumstances that make something *worthy* of trust. Data-driven digital environments that can learn about their users and, moreover, can dynamically be adjusted based on what they learn, are precisely the types of (digital) environments that can *engineer* trust by finding out what it is that makes users trust something and change (elements of) the digital environment accordingly to evoke (a psychological state of) trust. The resulting trust

---

69 (Lele, 2003)

70 (Wiesemann 2017)

71 Baier speaks of "special vulnerability" in this context: "If part of what the truster entrusts to the trusted are discretionary powers, then the truster risks abuse of those and the successful disguise of such abuse. The special vulnerability which trust involves is a vulnerability to not yet noticed harm, or to disguised ill will" (Baier 1986: 239).

72 (Nickel 2015, 552)

73 (Baier 1986; Hardin 1996)

74 (Nickel 2015, 559)

renders consumers vulnerable to the exploitation of that trust. So when consumers trust a digital service, one should always ask whether that trust is warranted, or merely the result of clever targeting.

(51) In the digital society it is thus especially clear that vulnerabilities typically originate in the *relations* consumers have with digital choice architectures, or with those implementing and operating them. Few consumers enter the digital marketplace as already vulnerable persons, simply by virtue of their personal characteristics. Most of the time, it is precisely people's ongoing involvement in various digital markets and services that render them *increasingly* dispositionally vulnerable to having their (economic) behaviour manipulated. The longer the relationship between a consumer and a digital service or app persists, the more the app or service establishes a position of power as a result of increased knowledge about its users. Vulnerability, in sum, should not be seen as a (semi-)static *property* of a person that exists independently of a person's relation to their environment; quite to the contrary, it is *precisely* a person's dynamic relationship to their environment that causes them to move in and out of states of vulnerability, depending on the circumstances. To the extent that these circumstances are (largely) controlled by sellers – as is the case in contemporary digital choice architectures: they occupy a key position which allows them to identify (or even evoke) and exploit vulnerabilities.

(52) Some examples might help illustrate the need for and use of the proposed conceptual refinements. Consider, for instance, health apps. Nearly all the widely used health and lifestyle apps are for-profit services (MyFitnessPal, Headspace, Strava, to name but some) which operate as *freemium* services. These apps can, in principle, be used for free, but app providers do try to build ongoing and profitable relationships with users. Users that keep coming back to an app can be profitable for a variety of reasons: the more users continue to use an app, 1) the more advertising can be sold, 2) the greater the chances that, somewhere down the line, users can be seduced to pay for additional (premium) services, and 3) the more user data can be collected, which can be sold to third parties or can be used to reinforce 1) and 2). In the health app context, there is usually a promise that the more a consumer uses an app and the better the app can 'get to know' the consumer, the better the app will be able to support (or empower) the consumer in their pursuit of a healthier lifestyle. Users are basically asked to trust a health app to serve users' interests, and volunteer access to their data as well as their decisional sphere with the promise of receiving support for healthy lifestyle endeavours. Now, to be sure, such relationships between health apps and their users can be empowering and helpful to users. At the same time, however, these relationships also introduce all preconditions for digital vulnerability by virtue of being *ongoing* relationships where health apps learn more and more about their users' patterns of behaviour and psychology. Health app providers can find themselves in a serious position of power, where a user has trusted them with privileged insights into their behaviour and psychology to be helped with some aspect of their health. Such a position of power also

grants health app providers the ability either to identify existing vulnerabilities of their user or to render their users vulnerable to commercial practices that *exploit* their privileged position of power. What emerges is a thin line between, on the one hand, collecting user data (often health-related) to help or support users, and, on the other hand, exploiting user data to target vulnerabilities for financial gain.

(53) Another example is gaming apps. Consider, for instance, Pokémon Go, which is in principle free to play. The game experience is carefully optimized for and geared towards so-called microtransactions; very small financial investments (typically a few euros or dollars) to acquire access to virtual items or events. Games like Pokémon Go are designed to 'hook'(Eyal 2014) users, by having them store value in the game (in this case building a collection of Pokémon) and by offering both recurring and variable rewards for coming back to the app (in this case better items and chances to catch better Pokémon). As users continue using the app for longer periods of time – that is, engage in ongoing *relationships* with the app – the app will be able to collect increasing amounts of user data to learn how the microtransactions system can be optimized. Users' vulnerability to commercial influences that promote microtransactions, again, is premised on the existence of ongoing relationships between users and gaming apps.

(54) As both examples show, an important *relational* dimension attaches to digital vulnerability.

d) Vulnerability as lack of privacy

(55) As has become clear, the data-driven nature of contemporary choice architectures contributes to their potential to exploit consumer vulnerabilities. In the digital society, the ability to collect and analyse user data contributes significantly to sellers' position of power. Limiting access to (user) data that help sellers learn about consumers can limit sellers' ability to identify or evoke vulnerabilities which can then be targeted. If we understand privacy as people's ability to control access to those things – places, decisions, as well as information and data – that are important to them, then privacy can be understood to function as an autonomy-enhancing value.[75] Privacy can function as a kind of 'shield' around consumers, protecting them from data practices that may weaken their own position of power vis-à-vis a seller.[76] Lack of privacy does not *of itself*, strictly speaking, constitute vulnerability. Rather, the overall lack of privacy that consumers experience fuels precisely those data-driven practices that promote exploitation of vulnerabilities. At the same time, (centralised) control

[75] (Rössler and Glasgow 2005)

[76] (Calo 2017)

over consumer data can result in new accumulations of market power and power imbalances.[77]

(56) To address lack of privacy as a potential source of vulnerability, lessons can be learned from the GDPR.[78] Specifically, Article 9 on the processing of special categories of data is interesting in this regard. By imposing more stringent rules on the processing of data that are considered to be especially sensitive (for instance data encoding racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, and health data, and data concerning one's sex life or sexual orientation) vulnerable individuals or groups are afforded additional protection. Interestingly, and highly relevant for this study, the European Data Protection Board (EDPB) has stipulated that situations in which advertisers use knowledge of the vulnerabilities of data subjects for targeted messages can fall under the prohibition of automated profiling in Article 22 GDPR.[79] Maglieri & Niklas have suggested that vulnerability should also play a role in Data Impact Assessments and obligations to privacy by design.[80] Although the GDPR's role in addressing (digital) vulnerability is worth exploring, it also should be mentioned that the 'special categories of data' approach suffers from the same outdated outlook on what makes people or data vulnerable and worthy of (additional) protection. The idea that one can distinguish between types of data that are inherently sensitive versus types of data that are *not* inherently sensitive mirrors the outdated approach of ascribing vulnerability to a subset of persons based on a set of predetermined personal characteristics (i.e., age, and physical or mental fitness, to name but some).

4. Implications for consumer law and policy

(57) The current approach towards vulnerability in Article 5 (3) UCPD is outdated and not particularly useful in addressing the situation of the digital consumer. Singling out and labelling particular groups of consumers as vulnerable by considering all other digital consumers as 'normal' is also not in line with our findings that digital vulnerability is essentially a universal condition that potentially applies to all consumers in the digital marketplace. What is more, the current approach tends to perpetuate the status quo, and is therefore also not particularly helpful from a consumer law and policy point of view.

---

77 Art. 29 WG: power imblance as source of vulnerability: Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, 10.

78 (Malgieri and Niklas 2020)

79 (EDPB 2020, 24)

80 (Malgieri and Niklas 2020)

(58) We have argued that digital vulnerability is inherently *relational* and *architectural* in nature and results from power imbalances between consumers and sellers: consumer vulnerabilities can be identified and/or created because consumers interact with sellers within digital environments that can *learn* about them and be *adapted* accordingly. Given the data-driven nature of contemporary digital commercial practices, every consumer is *dispositionally* vulnerable to being profiled and targeted exploitatively. For consumer law and policy, this means that instead of labelling certain groups or individuals as 'vulnerable' or non-vulnerable on the basis of some (semi-) permanent personal characteristic(s), the focus should shift to the properties and commercial practices of digital choice environments that can render everyone (dispositionally) vulnerable under the right conditions. Or, as Cole suggests: 'Vulnerability has to be reframed as a claim about injustice'.[81]

(59) A renewed, more universal perspective on consumer vulnerability involves a range of important implications for law and policy. First, establishing that the (dispositionally) vulnerable consumer is the norm, rather than the exception, translates into a conceptual shift and a new focus on identifying and declaring those practices unfair that exploit vulnerabilities and power asymmetries, thereby leading to situations of unfairness and inequality. If we all are vulnerable in principle, the real question is not so much whether we are vulnerable, but when digital technologies are used to single us out and (ab)use our inherent vulnerabilities to make us take decisions that we would otherwise not have taken. This also means that the fact that (almost) every consumer is rendered dispositionally vulnerable by contemporary digital commercial practices is not enough to speak of an unfair commercial practice. The real unfairness only begins when a seller decides to target those *dispositional* vulnerabilities in order to *actually* adversely influence – or: distort as a result of competition – the behaviour of consumers (in this sense also Duivenvoorde, and Calo who suggests a distinction between making vulnerable, and exploiting vulnerabilities). A dispositional vulnerability then becomes an occurrent vulnerability, which is where the actual unfairness is introduced.[82]

(60) For consumer law in general, and UCPD in particular, this means that Article 5 (3) UCPD is not the right frame to help us identify unfairness in the digital marketplace. Of much more theoretical and practical interest alike is the question whether the provisions of the UCPD that prohibit unfair commercial practices are able to guarantee that consumers are treated fairly, and declare unlawful the abuse of institutional and structural advantages that some firms have vis-à-vis the vulnerable consumer. Chapter 3 will look into this question in more depth. In so doing, it is worth exploring potential synergies with the GDPR. As Malgieri and Niklas have pointed out, the potential of data-driven commercial practices and digital choice

---

81 (Cole 2016, 273)

82 See also Art. L-122-8-L-122-10 French Code de la Consumation (*abus de faiblesse*) which defines abuse of vulnerability as an unfair commercial practice.

architectures to exploit dispositional vulnerabilities should also play a role in Data Protection Impact Assessments and Privacy by Design. Both are elements of professional diligence that could then, again, inform interpretation of Article 5 (1) UCPD. More generally, one could argue that the act of creating digital dependencies and asymmetrical (power) relationships, and the resulting influence over autonomous choices also creates new professional duties and obligations of professional diligence in the sense of Article 5 (1) and (2) UCPD.[83]

(61) The implications of a new conception of consumer vulnerability go beyond the need to rethink protection of the individual consumer. So far, under the liberal market model, large commercial tech platforms have enjoyed ample room to shape the digital marketplace. Within the confines of the GDPR and competition law, they were essentially left free to build digital choice architectures and a flourishing app economy. The underlying premise was that the laissez-faire approach in a prospering digital marketplace favours the average consumer, who – empowered through choice and information – will maximise their welfare. The role of consumer and data protection law in that context is to further empower the consumer and help them play an active role in the marketplace. The reality, as we demonstrated, makes the 'average consumer' a rather unrealistic prototype. Digital marketplaces are characterized by structural power imbalances and choice architectures that are explicitly designed for exploiting individual differences and biases. Viewing these developments from a more universal vulnerability perspective teaches us that attempts at empowering users vis-à-vis digital platforms are futile as long as regulators do not also tackle the structural power imbalances and inequalities that manifest themselves in the architectures they create. And because these imbalances are structural as well as relational, so must be the solutions. Changing the defaults, opening up systems, giving consumers agency to influence decision paths, fighting lock-ins, abolishing data monopolies – in short, addressing vulnerability and bringing fairness into the digital market place is not simply a question of empowering consumers, but of changing markets.

(62) As a final observation, so far, the focus of our analysis has been very much on consumer law and the impact of certain digital market practices on consumers' economic decisions. It is worth mentioning that, in the digital society, the distinction between the consumer as economic actor and the citizen as social actor is further eroded.[84] The data that exists about us, as consumers, can be used to take (automated) decisions that affect us in different areas of our life, including politics and work. Consumption-related data are used to identify target groups for political campaigns, and data collected about the way people live their lives, such as data from fitness and life-style apps or social media, or how they inform themselves (data from media usage) are combined in unprecedented ways to be used outside the commercial

---

83 Spindler, arguing in favour of special fiduciary obligations, and other positive obligations (based on ethics), due diligence, (Spindler and Seidel 2018).

84 (Scammell 2000)

realm as well, to influence elections, screen employees, decide about insurance and social benefits. Governments combine 'citizen data' with consumption data (for instance in the field of credit scoring)[85] to engage in new forms of data-driven governance and public service provision.[86] In all these activities, governments often rely on the services of (large) commercial parties, often the same parties that are the main drivers behind commercial profiling and targeting strategies.[87] Ultimately, all these practices can also determine who gets access to which commercial/public services at what price, and who is refused access or is provided with access on less favourable conditions.[88]

(63) Consumer law, with its current focus on economic decision-making, is little prepared to deal with the broader societal implications of consumer vulnerability in other aspects of social life. Broadly, the same is true for data protection law, which very much focuses on concrete acts of data processing in individual cases, and the rights and concerns of individual users vis-à-vis digital market practices. Partly this is a result of the way the competencies between the EU and Member States are distributed, in combination with the strong economic focus of EU law. Partly, this gap of addressing the more societal implications of consumer vulnerability is the result of a gap in our legal framework – a gap that needs addressing (see section III. (4) b)).

Chapter II. Consent and post-consent data management in EU data and consumer protection law

1. Empowerment through information: the current information paradigm

(64) Currently, we are observing a movement in law and policy making towards greater consumer empowerment online.[89] In fact, agency of internet users is one of the central objectives of the General Data Protection Regulation (GDPR) introduced in the European Union. The Regulation aims at giving consumers a high degree of control over their data online, allowing them to protect their privacy. One of the main empowerment mechanisms currently employed in practice is the so-called 'notice and choice mechanism'. First, consumers are informed about data collection, storage and processing through an information statement (in a consent notice or privacy policy) and subsequently they are invited to agree directly or

85 (Pasquale and Citron 2014)

86 (Dencik et al. 2019)

87 (Dijck, Poell, and Waal 2018)

88 (Solon Barocas and Andrew D Selbst 2016; Ray Fisman and Michael Luca 2016)

89 (Boerman, Kruikemeier, and Borgesius 2017)

indirectly.[90] Consent given by informed consumers must help them to exercise their right to informational self-determination, meaning that each consumer, having sufficient information, should be able to determine for themselves how their personal data is shared with others.[91]

(65) The requirement to inform consumers before they consent to data collection, storage and processing is one of the obligations for data controllers mandated by the GDPR. More specifically, the Regulation tells us that meaningful consent can only be given after a person has been properly informed, and the GDPR includes requirements specifying what 'properly informed' actually means. Article 12 GDPR specifies *how* information should be provided to a consumer. It has to be given in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information specifically addressed to a child. The information should be provided in writing or by other means, including, where appropriate, by electronic means. 'Intelligible' means that it should be understood by an average member of the intended audience.[92] Regarding the language used, 'information should be provided in as simple a manner as possible, avoiding complex sentence and language structures'.[93] In Articles 13 and 14 GDPR, guidance is given on *what* information should be provided. The regulation specifies that consumers need to be informed about:

1. the identity and the contact details of the controller and, where applicable, of the controller's representative;
2. the contact details of the data protection officer, where applicable;
3. the purpose of processing for which the personal data are intended as well as the legal basis for processing;
4. whether processing is based on legitimate interests pursued by the controller, or by a third party;
5. the recipients or categories of recipients of the personal data, if any.

(66) In addition, the ePrivacy Directive requires that users are provided with clear and comprehensive information on the placing of cookies or other forms of digital technology designed to store information or to gain access to information stored in the terminal equipment of a subscriber (such as cookies). In this case, users also need to be informed about the purposes of the processing and are offered a right to refuse cookies (Article 4 (3) ePrivacy Directive).

---

90 (Nouwens et al. 2020)

91 (Westin 1968)

92 WP29 'Guidelines on transparency', p. 7.

93 WP29 'Guidelines on transparency', p.9.

(67) At the same time, paragraph 2 of Article 12 GDPR also sets the requirement to inform consumers about their post-consent rights, such as the Right of Access to Data, the Right to Data Portability, and the Right to be Forgotten. First, the Right of Access to Data guarantees consumers the right to request a copy of any of their personal data which are being processed (this includes information on what data is being processed and for what purposes, on recipients of the personal data to whom the personal data has been disclosed as well as information on the retention period of the data). Second, the Right to Data Portability enables consumers to obtain their personal data from a controller in a format that is easy to reuse in another context, and to transmit the data to another controller. That way, consumers can choose without hindrance the party that will process their data. Third, the Right to be Forgotten gives consumers the right, under certain circumstances, to have their data erased by the controller without undue delay. These three rights form the basis of consumer post-consent management possibilities.

(68) Practical implementation of the requirements described above is visible to consumers in the form of privacy policies, cookie and consent notices. Websites that collect, store and process data usually offer consumers the required information in privacy policies, which are legal documents meant to inform readers how data are collected, stored and processed (including potential sharing with third parties) but also to meet the legal requirements of informed consent and subsequently protect the company against privacy lawsuits.[94] In the online advertising industry, which collects and processes large amounts of data, the Transparency & Consent Framework by IAB Europe is one of the most common examples of fulfilment of GDPR requirements. This is an 'industry tool that supports companies within the digital advertising ecosystem as they manage their compliance obligations under the GDPR and ePrivacy Directive'.[95] However, the tool is widely criticized for lack of transparency regarding post-consent data management and not providing granular consent, but bundling purposes instead.[96]

(69) Along these lines, empirical research in social and behavioural science also points to a number of possible challenges to the information and choice paradigm. According to the Theory of Informed Consent, individuals are able to consent to something once they have received information, have understood it, and have explicitly expressed agreement.[97] This means that even when all information requirements have been met, informing consumers may not be an effective mechanism for empowerment and achieving informed consent due to lack of understanding and lack of ability to make rational consent decisions. In fact, social

94 (Metzger and Docter 2003)

95 (IAB 2020)

96 (Ryan 2018)

97 (Faden, R. R and T.L. Beauchamp 1986)

scientists have debunked many of the assumptions of human decision-making on which the empowerment through information mechanism is based.[98] Such findings question the effectiveness and appropriateness of the information and consent requirements of the GDPR, but can also inform law and policy makers about how to make informed consent mechanisms more effective.

(70) Thus, looking at the information and choice paradigm and requirements set out in the GDPR from the perspective of consumers, the question arises to what extent they are an effective empowerment mechanism both at the time when consent is given and later, regarding post-consent data management. To answer this question, this report analyses three main research questions:

- *RQ1*: How can consumers be meaningfully informed about technically complex issues such as data collection online?
- *RQ2*: How realistic is an informed consent approach in times of information overload and constantly divided attention?
- *RQ3:* What role can GPDR and consumer law play in helping consumers to manage their data once consent has been given (post-consent)?

(71) To answer these questions, we first discuss challenges to the information paradigm from the perspective of consumers and building on insights from the empirical literature. In so doing, we also consider the changing character of the consumer-trader relationship in digital marketplaces, and in particular the relational aspect and temporality of the relationship (instead of one-off transactions, see also section 1 on vulnerability). In other words, we also explore what the insights from empirical research tell us for the temporal dimension of the information paradigm. Based on the challenges identified, possible solutions are discussed and suggestions made as to how the information and consent requirements of the GDPR could be complemented by other mechanisms and legal frameworks, such as EU consumer law to protect consumers from entering into risks of undefined scope and to avoid burdening the consumer with voluminous policy information, as well as overload by managing consent(s).

a) The consumer perspective

(72) Informing consumers in accordance with current legal requirements and subsequently asking them for consent to data collection, storage and processing may yield a legally valid basis for such activities. However, this does not guarantee the effectiveness and meaningfulness of these mechanisms. The current information and choice paradigm is strongly rooted in information provision through disclosures. For disclosures to fulfil their role, they not only have to be complete and meet legal requirements, but it is also important

98 (Ariely 2008; Kahneman 2012; Thaler 2015)

that consumers are motivated to read them, and once they do so, they need to be able to comprehend them.[99] This means that both consumer-related factors (motivation, knowledge, biases) and disclosure-related factors (informativeness, completeness, comprehensiveness) impact the effectiveness of the current information paradigm. These consumer- and disclosure-related issues are discussed in this section from a social and behavioural science viewpoint, offering insights into challenges related to the advancement of technology, individual biases and issues stemming from the actual fulfilment of information requirements in privacy notices.

b) The technological complexity perspective

(73) From the technological perspective on data collection, storage, and processing, four main issues arise related to the rapid progress in this field and its subsequent complexity. First, how data is processed is constantly evolving with new technologies being developed, which makes it difficult to provide consumers with the necessary information in the first place. The complexity of technology also makes it difficult for consumers to understand the technical architecture behind online information flows.[100] They are often not aware of what data is collected, or by whom, and how it can be used and shared with third parties. This gives the consumer a feeling that data collection and processing online is creepy and out of their control.[101] Nowadays, personal data can be aggregated and analysed on an increasingly vast scale and over longer periods of time.[102] This aggregation of data is in fact more important to the industry than individual datasets about consumers. They allow for analysing data merged from different sources to discover unexpected relations and patterns, which may not be what consumers expect from post-consent data processing. Using data beyond the scope of the original consent is often referred to as 'context creep', meaning the data is re-contextualized, which in turn makes it basically impossible to truly inform consumers about the consequences of granting consent and for consumers to be fully aware what giving consent for data collection and processing may mean in the long run. Future combinations and uses of data are unforeseeable for the consumer at the consent stage regardless of their competences.[103]

(74) At the same time, the current digital landscape is more complex and more opaque than ever before. On the one hand, it becomes ever more complicated due to frequently changing privacy policies that involve numerous third parties with their own policies.[104] On the other

---

99 (Milne, Culnan, and Greene 2006)

100 (Matzner et al. 2016)

101 (Ur et al. 2012)

102 (Custers et al. 2018)

103 (Matz, Appel, and Kosinski 2020)

104 (Matz, Appel, and Kosinski 2020)

hand, the current 'agile turn' in digital services raises additional questions about understanding among consumers. According to the new agile ways of working in the digital industry, many services available to users (that they give their consent to) are in fact unfinished products needing further optimization. This means that services and software are not designed to be end-products, but are brought out to users in a modular way, designed to evolve based on architecturally integrated optimization features feeding on user data.[105] Thus, in addition to technological complexity, the new ways of working in the digital industry lead to technology that is inherently open-ended and unpredictable in terms of its functioning and development in the near future. Even having sufficient knowledge and understanding, the consumer cannot predict what will happen to their data and what possibilities it gives the processor post-consent.

(75) Furthermore, from the perspective of the consumer, understanding not only what will happen to the data once consent has been given, but also having understanding and control over certain types of data that is being collected online is problematic. Much data is being generated without the individual being aware of it. For example, cell phone location data or biometric data collected by smart devices such as fitness trackers are rather abstract to the consumer, who will often be unaware that such data are being stored and processed for different purposes.[106] Such data are in fact too abstract and technologically complex for users without additional training to understand. However, even more common and by now long-established data collection methods such as using tracking cookies on websites pose challenges to consumers who have been shown to believe that cookies save their browsing history and are person-based.[107] Thus, being able to fully understand data collection requires consumer-related factors, such as digital literacy, that cannot automatically be assumed.

(76) Finally, due to technological progress and the development towards aggregating data on a large scale, the current notion of information and consent becomes outdated as it is focused on individual consent for processing data, while the consequences of such consent often also affect others. Information gathered from consenting individuals can be used to profile other individuals with similar observable characteristics and it is not necessary for these individuals to give their consent. In fact, when enough consumers consent to the collection and processing of their personal data, it is possible to infer missing values of other people.[108]

105 (Hoboken and Gürses 2018)

106 (Custers et al. 2018)

107 (Smit, Van Noort, and Voorveld 2014)

108 (Custers 2016)

c) The individual biases perspective

(77) It is not only challenges stemming from the complexity of technology and the sheer volume of big data being collected online that form an impediment to the information and choice paradigm but also biases stemming from human nature. Extensive analysis of such biases can for example be found in the works of Zuiderveen Borgesius or Acquisti.[109] In this section, we discuss three biases that showcase this impact of human nature specifically on consumer empowerment.

(78) First, the timing when information is offered to consumers is crucial for their decision-making. In fact, consumers get the information when they do not need it (visiting a website or downloading an app when their objective is to complete this action). At the moment when the information is presented to consumers, their objective is not to protect their privacy, but to access the information or services that ask them to share their personal data. Consenting to data sharing, storage and processing thus often carries certain immediate benefits (such as convenience or access to information). The risks of disclosure are usually only felt much later. This situation leads to so-called 'present bias', meaning individuals disregard future costs when they can choose immediate gratification.[110] For example, Wang and colleagues[111] found that users of social networks may gain some immediate pleasure from posting a selfie, but would often end up regretting it later. They evaluate the disclosure decision differently once they experience both the short-term and long-term consequences.

(79) Additionally, as Utz, Degeling, Fahl, Schaub and Holz[112] have shown, a common motivation for giving consent is the assumption that such consent is required to access the website. Consumers' objective is to access that website, so they in fact feel that they do not have an actual choice. They consent to disclosing data with incorrect information and without the necessary understanding of how their data will be processed in the future and what the actual implications of their consent decision are. This is particularly important as many digital service relationships are not one-off situations in which the relationship finishes as soon as the user leaves the website, but they form a long-term service relationship that evolves over time. In such an evolving relationship, once consumers experience both short- and long-term consequences of disclosure, they may need additional information (for example when they want to examine the conditions of data collection or change their consent decision), but they often do not know where and how to get it.

---

109 (Acquisti, Brandimarte, and Loewenstein 2015; Zuiderveen Borgesius 2014)

110 (Acquisti and Grossklags 2005)

111 (Wang et al. 2011)

112 (Utz et al. 2019)

(80) The way consumers are offered information according to current legal requirements not only has temporal consequences, but the information paradigm may also have unexpected 'side effects' for consumers, in the short and medium term. Social scientific research on information and privacy behaviours has shown that offering consumers additional information and safeguards, for example in the form of privacy seals, makes users feel more secure and less protective of their privacy.[113] Along these lines, in the context of online disclosure, Brandimarte, Acquisti and Loewenstein[114] introduced the notion of a control paradox that is important for understanding the effectiveness of the information paradigm. It tells us that perceived control over sharing private information increases willingness to publish sensitive information. More specifically, they conducted a series of experiments in which they manipulated the participants' control over information disclosure, but not their control over actual access to and processing of data. Their findings point to a paradox: more control over disclosure decreases one's privacy concerns and increases willingness to disclose information, even when the probability that strangers will access and use that information stays the same or, in fact, increases. In the context of the information and choice paradigm, Strycharz, Helberger, Smit and van Noort[115] concluded that such a paradox also takes place in the context of the transparency requirements set by the GDPR. Receiving information on data collection, storage and processing and their rights, consumers feel that consenting to data collection is less risky. Thus, transparency has unexpected side-effects that may put consumers' vigilance to sleep and push them towards taking more risks when consenting to data collection.

(81) Regarding how consumers make the decision to consent to their data being collected, it has been commonly argued that they weigh risks and benefits before they make a decision, which can be described as the privacy calculus.[116] The most important reason why people consent to their data being collected online are the expected benefits that include, for example, entertainment, tailored information, or access to information.[117] At the same time, the perceived costs also play an important role and include, for example, loss of control or privacy. Consumers need full information about the intended data processing to make such a calculation. A recent meta-analysis has confirmed that this calculation takes place as costs such as privacy concerns and perceived risk negatively impact information disclosure.[118] However, calculating the costs and benefits of consenting to data collection rests on the assumption that consumers always have a choice between using or not using a service and

113 (Noort, Kerkhof, and Fennis 2008)

114 (Brandimarte, Acquisti, and Loewenstein 2013)

115 (Strycharz et al. 2019)

116 (Laufer and Wolfe 1977)

117 (Bol et al. 2018)

118 (Baruh, Secinti, and Cemalcilar 2017)

full information about what the actual costs and benefits are. In the digital, constantly connected, society consumers have to deal with 'new pressures to perform [them] self online in order to just function as a social being'.[119] Sharing data and leaving digital traces has in fact become a constitutive element of being a digital citizen, and engaging in social, political and economic practices.[120] As a result, consumers often have to engage with certain services or are even dependent on them in order to achieve their goals (such as staying connected to other people or accessing information they need). This pressure puts into question to what extent they can use the information they are provided with and exercise a cost-benefit analysis when consenting to data collection. This is particularly true of individuals more susceptible to social pressure such as adolescents and young adults who have been shown to have heightened responsivity to such pressure across domains.[121]

d) Impact of formulation of notices

(82) While technology (*what* information) and human biases (*to whom*) impact the effectiveness and appropriateness of the information and consent paradigm, also of great importance is *how* the information is presented. While the GDPR provides some guidance on formulation of privacy notices, it leaves room for interpretation. This is reflected in practice: the notices that consumers see on different websites vary widely in terms of the user interface, their functionality, content and formulation. Some only display information to visitors, while others include complex opt-in choices and actually block cookies until consent has been given.[122] Research in social sciences and humanities points to three main issues related to formulation of information, namely its comprehensiveness, framing, and application of so-called 'dark patterns'.

(83) First, in general, privacy notices are long and difficult to understand: even experts find them misleading. For example, Cranor[123] estimated that it would take a user 244 hours a year on average to read the policies of every website they visit. As Milne and colleagues already argued in 2006, privacy policies need to be assessed on readability to make sure that they are understandable to a large proportion of the population. Along these lines, in a recent ruling of the Court of Justice of the European Union (CJEU/Court of Justice), Advocate General Szpunar gave the opinion that when speaking in terms of informed consent we should think of the consumer as the average European consumer who is reasonably well informed and reasonably observant and circumspect and who is able to take the decision to

119 (Couldry and Hepp 2016, 60)

120 (Van Dijck 2014)

121 E.g. (Steinberg and Morris 2001)

122 (Degeling et al. 2019)

123 (Cranor 2012)

make an informed commitment.[124] Thus, notices need to be readable and understandable to 'the average European consumer' or alternative mechanisms are needed. This leaves a number of questions open and unanswered such as what are reasonable expectations of the average consumer, who is the average consumer in terms of informing people about technologically complex issues, and does the average online consumer even correspond with the average offline consumer? Moreover, these insights also further emphasize the reflections on consumer vulnerability from the first sections, and issues related to information asymmetries that can result in states of structural, universal forms of vulnerability.

(84) Second, as Matzner and colleages argue: 'The reasons for not using a service or product are usually buried deeply in license agreements or privacy policies we have to 'consent' to before using. The reasons to use them, on the contrary, are promoted by the best advertising agencies in the world'. [125] How the information provided to consumers is framed impacts their decision-making: the way the notice is presented, namely as either a good thing or a bad thing, impacts consumer behaviour. Positively framing a consent notice as more protective of consumer privacy will lead to a stronger intention to consent.[126] Framing is often used by websites in consent notices that establish the positive implications of consenting to data collection (access to various functionalities or improved experience), while such notices ignore or downplay the possible negative consequences. The linguistic patterns in privacy policies also show that while they should aim to fulfil the information provision, they in fact can tend to 1) downplay the severity of data collection by using such words as *carefully* or *occasionally;* 2) obfuscate the reality by taking away consumer agency and underlining that the consumer is the *receiver*; 3) focus on building a relationship and not purely informing by using first- and second-person pronouns, and 4) include persuasive appeals such as comparisons to others (*like, most*) or negative propositions.[127] These framing and linguistic mechanisms show that privacy policies can walk a precarious balance between aiming to inform consumers in order to fulfil the information provision, or convincing consumers to consent. More research is warranted into the framing of consent notices and the effects on informing consumers and consumer choices.

(85) Third, the cognitive biases of individuals described in the previous subsection can and are being used by websites to increase consent: 'Cognitive biases make rationality difficult and so-called 'dark patterns', or design tricks platforms use to manipulate users into taking actions they might otherwise have not, weaponize the design of built online environments

---

124 European Court of Justice, Case C-673/17 (*Planet49*).

125 (Matzner et al. 2016, 297)

126 (Adjerid et al. 2013)

127 (Pollach 2005)

to harm consumers and their privacy'.[128] Such 'interface design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make'[129] make disclosure 'irresistible' by connecting information-sharing to certain benefits. In general, privacy notices tend to provide too few options, giving visitors the impression that the choices they make are not meaningful, leading to the habit of clicking any interactive elements of these notices to make them go away. Of the most popular websites in the EU, 57% use such interface design choices to steer visitors towards giving their consent.[130] Such choices include using suggestive colours for the button to accept defaults, hiding further privacy settings behind hard-to-see links, and preselecting checkboxes that consent to data collection. This way, designers intentionally make it difficult for users to make informed privacy decisions. Utz and colleagues[131] showed that seemingly small decisions on design and content of consent notices (position in a website or framing) could substantially impact if and how people interact with consent notices. More specifically, they concluded that visitors were most likely to interact with notices placed at the bottom left position in the browser while bars at the top lead to the lowest interaction rates. This is caused by what content lies behind the notice – if the content obstructed by the notice was important to the visitor, it would encourage interaction. Also, the more options a notice provided, the more interaction it received. This goes in line with the assumption that notices with single choices to consent give the user a feeling that their choices are not meaningful, which lowers motivation to protect privacy by making use of consent functions.[132]

2. *Post-consent data management from a consumer perspective*

(86) What and how information is given to consumers at the moment of consenting to data collection and processing is crucial for their being able to give informed consent at that particular moment. This information concerns both immediate and long-term consequences. Indeed, one of the requirements for valid informed consent is that the person giving consent should not only be informed about what they are consenting to, but should also be made aware of what future consequences such consent may have.[133] Post-consent data management, that is, the question of what will happen to the data once it is collected and what control possibilities individuals have is thus crucial to the information and consent

128 (Waldman 2020, 105)

129 (Mathur et al. 2019, 1)

130 (Utz et al. 2019)

131 (Utz et al. 2019)

132 See Strycharz et al. 2019 for a study on the impact of efficacy of opt-out options on protection motivation and behaviour.

133 (Custers et al. 2018)

paradigm. Two circumstances characterize such post-consent data management. On the one hand, it concerns rights of users regarding their personal data once consent has been granted. Article 13 GDPR clearly requires data controllers to provide individuals with information about such data subject rights. On the other hand, it also concerns transactions that are no longer one-off, but have a longitudinal character (downloading and consenting to terms of an app that will be used over a long period of time). This raises questions about how this longitudinal and relational character can be considered in terms of post-consent transparency. Thus, issues stemming from technological complexity, individual biases, and the way consent itself is given obstruct the effectiveness of post-consent management in both contexts. The mechanisms behind it will be explained in this section.

a) Post-consent transparency management: a technological complexity perspective

(87) Technological progress made in data processing not only impacts the appropriateness of the information paradigm, but also individual possibilities for post-consent transparency management in terms of further possible uses of data. Practices in which anonymous aggregated datasets can be used may have long-term consequences for individuals. These consequences may be difficult to foresee at the moment of consent. In fact, much of the data being collected online may be processed on an aggregated anonymous level, but can still be used to generate consumer profiles, which at a later stage will have an impact on the individual. This profile generation happens once consumers have already given their consent, and in fact they have little impact on it. As anonymous data are not regulated by the current post-consent mechanism (data subject rights to access, correction, deletion), post-consent management possibilities are limited, if existent at all. For example, a company can use data to determine different groups or types of buyers' willingness to pay. This relation can be established using anonymous aggregated data, but such correlations can ultimately have a serious impact on individuals, resulting in discrimination against certain groups.[134]

b) Post-consent data management: individual biases

(88) Looking at post-consent data management from the perspective of consumers, so-called privacy fatigue plays a central role in their behaviour and motivations. It arises from situations in which people are faced with heavy demands and inability to meet their goals.[135] In the current context, privacy information and consent requirements have become complicated and frequent enough that consumers feel that they are difficult to comprehend and that they are not able to ensure their online privacy when confronted with them. This leads to psychological stress and fatigue. One of the more common coping strategies in such

134 (Poort and Zuiderveen Borgesius 2019)

135 (Hardy, Shapiro, and Borrill 1997)

a situation is behavioural disengagement, which can be defined as 'reducing one's effort to deal with stressors, even giving up the attempt to attain goals with which the stressor is interfering'.[136] Privacy threats may lead to motivation to protect one's privacy consciously, but with a sense of fatigue consumers may not actively engage in privacy protection behaviours, such as the different possibilities they have to manage their data after giving consent.[137] While fatigue may thus play a role at the point of giving consent – disengaged consumers may not give their attention to information offered to them, and fatigue has an even stronger impact on post-consent data management – consumers may not be motivated to undertake any action once they have given consent and have the feeling that their actions are not meaningful in the first place.

(89) Next, to (lack of) motivation, trust in – and even more importantly the trustworthiness of – the intermediaries that collect data plays not only a central role in decisions regarding entering into a relation with an app provider (see section I (3) c), but also in post-consent data management. A trusting individual is willing to accept some risk and vulnerability towards others; Metzger[138] describes trust as a 'social lubricant' that mitigates perceptions of the risk involved in online interactions. Regarding online disclosure, consumers entrust their personal information to digital platforms (intermediaries and trustees) just as they entrust their financial information to financial institutions or medical information to doctors.[139] In this situation, consumers expect trusted persons to act for their benefit or, at least, not to act in ways that benefit the trusted person at the expense of the consumer. As described in section I (3) c), in the context of digital services, these are often evolving relationships. An illustrative situation is that of a provider of a fitness tracker or a news subscription, where trust can develop and increase over time, which can in turn reduce vigilance – again, over time. However, in the context of post-consent management, trust needs to be distinguished from trustworthiness. This means on the one hand that companies need to earn and retain the trust of consumers (and meaningful information requirements can play a role here). But it also means that because of the complexity of the technological environment and also the longitudinality of many consumer-service provider relationships, attempts to instil or engineer trust in such a relationship should come with additional fiduciary obligations on the side of the data controller, and abuse of trust a point of attention for the regulator.

136 (Carver, Scheier, and Kumari Weintraub 1989, 269)

137 (Choi, Park, and Jung 2018)

138 (Metzger 2006)

139 (Waldman 2020)

c) Post-consent data management: impact of temporal aspects

(90) Finally, the strong temporal aspect of the current information and consent paradigm is crucial to post-consent data management issues. Consent is usually asked when registering for a service, visiting a website for the first time, or installing an app, and is commonly not renewed afterwards even if the consumer keeps using the service and app and visits the website multiple times. Consent is given by the consumer while not their main objective (but they want to visit a website, see previous section). As a result, consent is given 'once and forever' regardless of whether it gets outdated due to technological developments or changes in consumers' lives.[140] This does not reflect the actual character of consent: in fact, it is not given, but the consumer experiences it as part of a dynamic process. As much as data collection, storage and processing is often represented in the industry as a process with different elements that influence one another (see The Cross-Industry Standard Process for Data Mining, an open standard process model conceived in 1996 under the European Strategic Programme on Research in Information Technology (ESPRIT); currently commonly used in the industry, it represents how data is collected, stored, and processed in practice[141]), consent should have similar qualities. Information needs, life situation, preferences of consumers – all these change. The burden is now on consumers to show motivation and take action in order to make sure such factors are reflected in the consent decisions they have made (by using their individual rights guaranteed under the GDPR such as the Right to Data Portability or the Right to be Forgotten). Changes to the current consent paradigm have been proposed to transform consent into a *process*. For example, Custers[142] has suggested including an expiry date for consent to reflect its temporal character. Due to the longitudinal character of the relation between data processors and consumers, the latter may not only need to have a right to withdraw consent, but also the opportunity to review consent, once given, on a periodic basis. Very practically this would imply that consumers should not only be informed before the actual transaction about their right to withdraw, but reminded periodically that they have the right to withdraw, and how they can exercise that right if the service or the data collection no longer fits their current needs or situation in life. However, while such solutions represent the longitudinal character of consent decisions, they do not offer a remedy for technical complexity or the impact of anonymous data processing on individuals.

---

140 (Custers et al. 2018)

141 (Larose and Larose 2014)

142 (Custers 2016)

3. *Improving the information paradigm*

(91) As demonstrated in the previous two sections, technological complexity, individual biases, and the characteristics of the information and choice paradigm itself negatively impact its effectiveness and applicability. In this section, we provide insights from social sciences and legal scholarship that can be used to improve the current paradigm both by lawmakers and by advocacy and education groups who aim to empower consumers.

a) Fostering protection motivation

(92) From a psychological perspective, managing consent to data disclosure online can be seen as a measure that consumers can take to protect their privacy. Past research into protection motivation has shown that for individuals to be motivated to take such measures, two main processes are crucial: the so-called *threat appraisal* and the *coping appraisal*. While the threat appraisal describes one's belief that the threat to privacy posed by online data collection is noxious (*perceived severity*) and that it is likely to happen (*perceived susceptibility*), the coping appraisal assesses belief in one's ability to protect oneself (*perceived self-efficacy*) and that the protective action is effective (*response efficacy*). Increasing these appraisal processes can motivate consumers to give informed consent in a conscious way (which would fulfil the assumptions of the information paradigm), but can be only achieved with sufficient effort both from companies that collect and process data and from regulators.

(93) For threat appraisal, while past research has shown that offering technical and legal information on the workings of data collection is not effective,[143] it suggests that offering information about risks stemming from data sharing may be more effective. Regarding how to offer this risk information, the impersonal impact hypothesis[144] provides suggestions as to how to activate threat appraisal in order to increase motivation. More specifically, it assumes that direct, lively explanations that really appeal to someone personally work better as a source of information than an explanation that is more broadly applicable to the heterogeneity of people. Translating this to the information paradigm, in order to successfully inform consumers, information should not be generic (as it is now in privacy policies), but **adjusted to personal experience and focused on potential individual risks**, by showing specifically what data are collected about them (for instance by showing which trackers collect personal data of consumers on the specific website they are visiting, as is currently possible through plug-ins such as Ghostery) and what the related risks are (specifying what privacy risks consenting to such trackers carries). Regarding technical complexity of data collection, while abstract explanations about the workings and

143 (Strycharz, van Noort, Helberget & Smit 2020)

144 (Tyler and Cook 1984)

consequences of data aggregation may not be effective, making consumers aware of **specific known outcomes** of data aggregation, based not only on their own but also on others' past decisions, could help them become more aware of related risks. Such personally relevant information would appeal to consumers' threat appraisal, demonstrating their susceptibility to data collection (seeing specifically what data is collected via, for example, a plug-in makes it apparent how data collection takes place or how data can be used through aggregation), which in turn would motivate them to make more informed choices. At the same time, information provided to consumers in privacy policies is complex and often not easy to understand. Past research on provision of information shows that for complex information visual material is more effective than textual material[145] and that the material should be adjusted to the needs of receivers. Thus, **personalized privacy notices**, in which the data collection practice is assessed from the perspective of a particular group of consumers,[146] will lead to more informed decision-making among consumers through increased threat appraisal and improved information provision. However, offering different consumers different information before asking them for consent also opens doors for abuse of information asymmetries that needs to be taken into account when personalizing privacy notices.

(94) Regarding coping appraisal, past research shows that in terms of privacy protective behaviours, it is not consumers' own efficacy that can motivate them to protect their privacy, but their belief in the effectiveness of the measures they are taking. Thus, effective **enforcement** of the current laws that give consumers the right not to give consent and thus guarantee the correct working of the information and consent paradigm is important for consumers to believe in the effectiveness of legal rules. At the same time, companies that collect data also have a responsibility to assure that consumers believe in the available tools. To overcome the current privacy cynicism, attitudes of uncertainty, powerlessness, fatigue and mistrust toward the handling of personal data by digital platforms[147] that make the consumer doubt the effectiveness of existing choice mechanisms, companies could provide consumers with **feedback** about the results of protective action. A direct message, showing that withholding consent means that no personal data will be collected, will contribute to higher perceived response efficacy and thus indirectly to more informed decision-making.

b) Training for effective protective behaviour

(95) Besides relying on information and current consent mechanisms, other practices focused on training consumers may be more effective in empowering them. They can in fact be seen as

145 (Meppelink et al. 2015)

146 See N. Helberger 2013 for in-depth disucssion on personalizing notices

147 (Lutz, Hoffmann, and Ranzini 2020)

a complement to the information and consent paradigm especially as consumers differ in their degree of understanding of current data collection practices.[148] One of these complementary strategies can be **training** based on inoculation theory.[149] This theory uses the biological metaphor of a vaccination to describe how a weak attack on one's attitude can help make a person immune to stronger attacks later on. Inoculation therefore consists of warning people about a threat and then teaching them how to deal with it. It thus involves showing consumers what data is being collected (by making them aware of different trackers), and then offering them training to teach them how to cope with it through, for instance, managing their preferences through consent notices. Thus an important part of this is showing and teaching effective behaviour. In such training, consumers are able to experience data collection and subsequently experiment with consent to see the impact of their decisions. Such training can complement the information and consent paradigm by 'preparing' consumers to cope with giving their consent consciously. Specific training intervention based on inoculation theory is currently being developed and tested at the University of Amsterdam.

c) Reducing privacy fatigue

(96) Privacy fatigue – a major threat both to the effectiveness of the information and choice paradigm as well as post-consent privacy management – requires additional action from the consumer after consent has been given. Psychological stress and fatigue and consequent disengagement have led to calls for more paternalistic approaches to privacy protection online, such as privacy nudges as argued for in recent legal research (Soh, 2019).[150] As fatigue is closely related to the sheer number of difficult and often unclear privacy choices a consumer has to make regarding their data (Choi, Park & Jung, 2018), it follows that reducing their number and complexity could contribute to reducing fatigue. This could be achieved by further **specification of how consumer data can be used**. More specifically, three such cases can be distinguished: prohibited data uses for which no consent is possible, legitimate data uses that do not require consent due to a statutory legal basis, and finally data uses that can acquire a legal basis through consent from the consumer. When consumers are asked for consent only in the third case, then on the one hand they benefit by way of protection from illegitimate data uses (which is what they expect from regulators[151]) and on the other hand they may perceive their choices as more meaningful and easier, which in turn may mitigate the feeling of fatigue.

---

148 (Strycharz et al. 2019)

149 (Banas and Rains 2010; McGuire 1964)

150 (Duivenvoorde, B.B. and CSECL (FdR) 2015)

151 (Strycharz, Ausloos, and Helberger 2020)

d) Design of notices

(97) Well-known are suggestions from scholars that have proposed a number of ideas on how to improve information provision through design alternatives such as colour coded labels.[152] However, more lately attention has shifted from visual alternatives and design solutions to suggestions how *not* to design consent notices, namely the dark patterns and other persuasive strategies mentioned in the previous section. For example, Utz and colleagues[153] showed that highlighting the 'accept' button in cookie notices leads to significantly less interactions with the notice compared to the situation when neither the accept nor the decline buttons are highlighted. Along these lines, offering a binary choice (one accept button) leads to less interaction from consumers compared to a list of choices. Similarly, positioning the notice in front of the central information on the page and not 'hiding' it at the bottom or top of the page leads to more interaction from users. Other tactics used by websites, such as framing underlying short-term goals which leads to dismissal of long-term consequences or using icons (such as a 'thumbs-up') to nudge users to consent can be expected to have a similar effect. Thus, insights from behavioural studies can inform law makers about **problematic design patterns** and how consent should *not* be given.

(98) In general, fostering data literacy or more general media literacy by offering the consumer adequate information regarding privacy risks, training, and feedback can still be a valuable tool for consumer empowerment in the shape of helping them to make more conscious consent decisions online. However, not including a broader social perspective and not addressing the inequalities of power and knowledge mentioned in this report renders this effort insufficient for protecting consumers in the online environment.

4. Improving post consent transparency management

(99) While improving the information and consent paradigm and supporting it by additional empowerment measures is important from the consumer viewpoint, making sure that inequality between data collectors and consumers does not arise once concern has been given is crucial. The control paradox described above highlights and reinforces the importance of post consent management and rights. This section proposes ways to offer consumers 'post-information' in the sense of ways to inform them about their rights once consent has been given.

---

152 (Kelley et al. 2009)

153 (Utz et al. 2019)

a) Momentary consent vs. consent as a process

(100) The way consent is given and evaluated should reflect that it is often part of an ongoing relationship. Post-consent management should consider the temporal character of consent decisions. Several recommendations can be made to reflect the process character of the information and choice paradigm. First, better **timing** of information and giving (or repeating) information at the right time is needed. Indeed, the consumer should be offered information at a time that is relevant in the consumer journey and their decision-making process. Offering information when the consumer for instance visits a website for the first time does not reflect this journey. As the consumer-service provider relationship evolves over time, more discussion is needed on possible post consent fiduciary obligations, for example inviting consumers to **review their consent** decision. Along these lines, the way information is provided at the time of first requesting consent and later when the relationship is established should be adjusted to the information needs and habits of consumers, which may change over time. To facilitate this, some scholars even suggest introducing an **expiration date** for consent.[154] Such solutions would remind consumers of their right to withdraw their consent. At the same time, they have to be executed carefully as they carry the danger of abuse of trust: data processors may abuse the trust that consumers develop in an evolving relationship by asking them to accept new conditions (such as in the context of an amendment to privacy policies).

b) Tools for consent as a process

(101) To make consent as a process effective in empowering consumers to take more control, attention is needed to tools that allow consent management over time. Currently, the Right of Access to Data, the Right to Data Portability, and the Right to be Forgotten are the only instruments available to consumers in this context. However, as argued above, they require substantial action from the consumer, which of itself may contribute to privacy fatigue. In order to overcome this fatigue, the tools instead need to have a low threshold for consumers so that longitudinal use does not actually lead to less motivation to use them. Social scientific research suggests that **visible and easily accessible** settings **across platforms** can help against 'consent overload' by lowering fatigue and improving consumer motivation (to one-off, but also continuous use). The *Sachverständigenrat für Verbraucherfragen* (SVRV), the German consumer dashboard, is an example of an accessible tool for post-consent management. Furthermore, to account for the technological complexity of data processing and possible future uses of (aggregated) datasets, information provided in such tools should not only concern data collection (as is the case with the three rights mentioned), but also **future possibilities**. While it is challenging for users to predict and understand future uses of

154 (Custers 2016)

their personal data, for post-consent data protection it is crucial to offer protection of data at all levels (importantly also including metadata) with a focus on what insights might be inferred from them.

Chapter III. Digital Asymmetry and Data Exploitation Strategies in Directive 2005/29/EC on unfair commercial practices

1. The benchmark: external-structural and internal-dispositional

(102) The legal analysis is based on the empirical findings and theoretical considerations from behavioural and communication science and legal philosophy in section 1. *Digital vulnerability* can be condensed in the distinction between the *external* structural impact on the consumer and their *internal* dispositional capabilities to handle the external structural impact. External structural impact covers the digitally mediated relationship, the choice architecture, the architectural infrastructure, and the knowledge gap. All these have in common that they are external to the consumer in that they result from the way in which technology is used and applied, from the knowledge gap on digitalization, from the sweeping line between their impact on the market behaviour of the consumer and their societal behaviour. Vulnerability is universal. Each consumer is confronted with *external* structural impact and therefore dispositionally vulnerable. *Internal* dispositional vulnerability refers to variations in individual capacities to deal with the external structure; they may be situational, informational, or source-bound.

(103) The distinction between external and internal digital vulnerability can be neatly translated into the UCPD through the concept of digital asymmetry. Section 2 provides the material against which digital asymmetry can be tested. The findings can be condensed in the formula of applied data exploitation strategies. Data exploitation strategies will be broken down at the ground level and the surface level. The ground level is the technological infrastructure; the surface level is visible in the document through which the technological setting is communicated to the consumer. It can be enshrined in a data privacy policy and/or in standard terms. The exploitation strategy forms an integral part of the ground level of the technological infrastructure and the surface level, the communication document. In the following we are using the notion of data exploitation strategy so as to test its legality in light of the UCPD.

2. The line of argument

(104) The most important tool for consumer agencies/consumer organisations and perhaps consumers themselves in the fight against data exploitation strategies consists in the rights

granted under the Directive on Unfair Commercial Practices (UCPD) and the Directive on Unfair Terms (UCTD).[155] These two directives aim at fairness in the market place and empower collective entities and consumers accordingly. The General Data Protection Regulation (GDPR) focuses on the rights and remedies of individual data subjects and on enforcement through data protection agencies. It combines data protection with the free flow of data in the Internal Market. Whether and to what extent fairness is enshrined in the GDPR and, if so, what kind of fairness, is subject to debate. The GDPR had left it to the Member States to grant consumer agencies/consumer organisations legal standing. However, this will change with the new Directive on Representative Actions, where the GDPR forms part of the list of consumer legislation that can be enforced by qualified entities.

(105) The *first* step is to integrate the distinction between external-structural and internal-situation impact into the conceptual and regulatory toolbox. The non-legal literature uses the notions of 'digital vulnerability' and 'vulnerability'. In European consumer law, vulnerability is a loaded term, like weakness. That is why this study proposes a different terminology that does justice to both dimensions of 'vulnerability', namely the external-structural and the internal-dispositional. The notion of *digital asymmetry* avoids both traps, i.e. the vulnerability trap and the weakness trap. Regulatory attention should shift from defining vulnerability or sorting out particular users under the concept of vulnerability towards tackling the sources of vulnerability, which comprise digital asymmetry.

(106) The *next* step is to qualify the overarching effect of data exploitation strategies from economy into society. Can a directive that is meant to protect the *economic* interests of consumers (Article 1) deal with the *societal* impact of the digital economy? The study does not investigate the question in full but points to problems resulting from a supranational economic legal order that is market-biased and based on the principle of enumerated powers. A second much more real problem derives from a recent reference of the German Bundesgerichtshof (Federal Supreme Court) questioning the applicability of the UCPD to data exploitation strategies as such.

(107) The analysis that follows is operating under the assumption that the Court of Justice will confirm the applicability of the UCPD – and maybe the UCTD – side by side with the GDPR. This immediately triggers the question of the interrelationship between the three: Does a particular data exploitation strategy which is to be held unfair under the UCPD also infringe the GDPR? Is the notion of fairness in both Directives the same?[156] If the data exploitation strategy is presented to the consumer as part of standard contract terms, the data exploitation strategy is submitted to the fairness test under the UCTD. The question then is

---

155 The two Directives oblige Member States to introduce an action for injunction, which can be granted either to consumer agencies or to consumer organisations, or to both.

156 (Clifford and Ausloos 2017)

whether and to what extent value judgements enshrined in the UCPD and the GDPR can or must be integrated into the fairness test under the UCTD.

(108) In a *third* step, the study is meant to advance the current academic and judicial debate through distinguishing between standardised data exploitation strategies and those which are tailored to targeting individual consumers. The study draws inspiration from the long-standing debate on judicial control of contract terms, which so far has been dominated by the distinction between standard terms and individually negotiated terms. We will show that both the UCPD and the GDPR follow in essence the same distinction between standardised and individualised data exploitation strategies. That is why we suggest deriving from that distinction a common ground of judicial control which cuts across all three pieces of legislation.

(109) Therefore, *fourthly*, we examine how data exploitation strategies leading to digital asymmetry are to be classified under the UCPD. The study defends and develops the hypothesis that external-structural asymmetries should be qualified as aggressive practices in line with Articles 8 and 9 UCPD. Legal problems abound in the information paradigm which governs consumer law as such and determines the scope and reach even of aggressive practices and the rather narrow legal requirements of the 'aggression test' under Articles 8 and 9, which seem to run counter to the distinction between standardised and individualised data exploitation strategies. That is why a further step is needed: the applicability of the general fairness test in Article 5 (1), in particular with regard to professional diligence. The study will argue that both routes are possible, but that the structure of the UCPD requires starting with an analysis of Articles 8 and 9 and using the general fairness test as a means of last resort.

(110) Classifying the external digital architecture of data exploitation strategies as an aggressive practice or as violating professional diligence does not in itself suffice to qualify them as unlawful. However, this categorisation allows us to justify shifting the burden of argumentation, if not the burden of proof, onto the 'user', who has to demonstrate that they do not collect and process data in an aggressive and/or unfair way. What remains to be solved is what exactly the supplier must demonstrate in order to show that its data exploitation strategy is not aggressive or not unfair. The study presents a set of criteria which could contribute to clarifying the standard of fairness.

(111) The last step is to break down the distinction between external/standardised and internal/individual vulnerability to the concrete facts of the individual case, thus to the situational circumstances where consumers are confronted with supposedly unfair data exploitation strategies, collectively through standardisation or individually by being targeted. Again, the parallel to judicial control of unfair contract terms may illustrate the difficulties which result from the multi-governance structure of the European legal order. In principle, the CJEU is not deciding on the facts of the case – not even in judicial control of

standardised terms or of blacklisted commercial practices in the Annex to the UCPD – but is interpreting EU law. Nevertheless, it is well known that the CJEU is doing exactly this, where the guidance given is so determinate that no leeway is left for national courts. However, the problem goes deeper. Is it suitable to have EU-wide prohibitions on certain unfair data exploitation strategies or should consumers even be able to consent to problematic practices *ex post*?

3. *Digital asymmetry: the legal concept*

(112) Language is telling. That is why it is politically and legally crucial to find the correct denomination for a legal concept to govern the monitoring and surveillance of the digital market and the digital society. This study takes a cross-cutting perspective, which investigates the UCPD, the UCTD, and the GDPR. In the law on unfair commercial practices, a long standing political fight has been under way over the use and usefulness of the 'average consumer' benchmark as the standard test and the vulnerability test as the exception to the rule.[157] In the law on unfair contract terms, such a clear cut divide does not exist. In its extensive case law the CJEU tends to refer to the 'weak' consumer who requires protection.[158] In the law on regulated markets, telecommunication, energy, transport and financial services, EU legislation builds on a distinction between the 'normal customer' and the 'vulnerable consumer'.[159] Unberath and Johnston have pointed to the divide between the average consumer benchmark in primary EU law and the weak consumer in most of secondary EU law.[160]

(113) In light of the complex history which stands behind the different consumer images, the concepts of both 'vulnerability' and 'weakness' are loaded. Both suffer from a legal and political burden. Linking the empirics of the digital economy and digital society to 'vulnerability' triggers misleading and counterproductive regulatory implications. Speaking of digital vulnerability, even if it makes sense in light of extensive research in behavioural and communication science, would misguide lawyers, in whatever function they are operating. Providing vulnerability with a meaning that overcomes narrowness and opens up to the external structural implications behind digital vulnerability seems difficult to achieve,[161] it would not do justice to the concept of vulnerability in the law on services of

157 (Howells, Micklitz, and Wilhelmsson 2006)

158 (Micklitz and Reich 2014, 771–808)

159 (Bartl 2010, 225–45; Johnston 2016, 93–138; Reich 2016, 139–58)

160 (Unberath and Johnston 2007, 1237–84)

161 Hacker 2020)

general interest and would not be in line with the concept of *universal* vulnerability proposed here.

(114) Similar objections apply to a potential concept of 'digital weakness'. The idea of the weak consumer insinuates the debate on power imbalance, which played a crucial role in the founding years of consumer policy. The difficulty so far has been to give power a normative meaning beyond the concept of 'abuse of power' in competition law and to some extent in contract law. The few hints on power imbalance in the case law of the Court of Justice[162] do not overcome the definition problem. The notion of 'exploiting a position of power' in the context of aggressive practices (Article 2 j) UCPD) is awaiting concretization in case law. Revitalizing weakness and making it the major benchmark might meet strong resistance in political and business circles, too. The average consumer has been celebrated as overcoming the weak consumer rhetoric in the law on unfair commercial practices. But there may also be resistance from the consumer side. No consumer would like to be qualified as 'weak', at least prior to a possible infringement leading to harm. Weakness has a pejorative undertone. It refers to someone who is not able to manage their consumption activities properly. This is also the reason why consumer lawyers insisted on the structural side of weakness in terms of imbalance of power and played down the internal dispositional dimension. However, these attempts did not really bear fruit in day to day practice.

(115) In order to do justice to both the empirical and theoretical finding and the loaded history of consumer images, it seems appropriate to look for a new concept that adequately covers what is empirically and conceptually discussed in non-legal research as 'digital vulnerability'. A variety of possible candidates suggests themselves – *digital inferiority*, *digital imbalance* and *digital asymmetry*. 'Inferiority' is only another word for weakness and suffers from the same reservations. Digital 'imbalance' brings us back to what imbalance means and first requires defining power, this time in the digital – not in the analogous – economy and society. It might make sense in terms of the GAFAs which are in the limelight for using competition law as a tool for controlling abuse of a dominant position,[163] but only for them. In light of these reservations, the concept of '*digital asymmetry*' seems more appropriate as it leaves space for interpretation beyond power imbalances, getting away from individual responsibilities of the 'stronger party' and putting emphasis on the *structural* effects of how the technology is used.

---

162 (Micklitz 2018, 329–31) with reference and discussion to the relevant case law of the ECJ with regard to collective agreements.

163 The Bundeskartellamt's decision prohibiting Facebook from collecting and using data from its subsidiaries and third companies for its own business activities caused a worldwide sensation. Now, the German Federal Supreme Court (BGH) reinstated in a summary procedure the prohibition order of the German cartel office, Beschluss 23.6.2020, KVR 69/19 http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=109506.

(116) A word of caution is needed though. In its famous 'suretyship judgment' the German Constitutional Court[164] held:

> Ist aber der Inhalt des Vertrages für eine Seite ungewöhnlich belastend und als Interessenausgleich offensichtlich unangemessen, so dürfen sich die Gerichte nicht mit der Feststellung begnügen: "Vertrag ist Vertrag". Sie müssen vielmehr klären, **ob die Regelung eine Folge strukturell ungleicher Verhandlungsstärke ist**, und gegebenenfalls im Rahmen der Generalklauseln des geltenden Zivilrechts korrigierend eingreifen
>
> If, however, the content of the contract is unusually onerous for one party and obviously inappropriate as a balance of interests, the courts may not be content with the statement: "contract is contract". Rather, they must clarify whether the regulation is a **consequence of structurally unequal negotiating power** and, if necessary, intervene to correct this within the framework of the general clauses of the applicable civil law (*emphasis added H.-W. M.*).

(117) This rather strong statement made in 1993 by one of the national courts in Europe whose judgments are followed attentively set an end to the most immoral types of suretyship contracts by family members. However, the concept of 'structurally unequal negotiating power' did not reach the daily court practice of judicial review of standard terms. In practice, the formula of unequal negotiating power was successfully substituted by the idea and ideology of '*information asymmetry*'. The doctrine of information asymmetry made its way into financial regulation and survived, although empirical research amply demonstrated that ever more information cannot compensate for asymmetry, not only in consumer finance[165] but more generally in consumer contract law.[166]

(118) Therefore, *digital asymmetry* will and may never be reduced to information asymmetry. Digital asymmetry is a structural phenomenon that affects all consumers and that cannot be overcome by providing ever more information. As the consumer is structurally and universally unable to 'understand' the digital architecture, information in whatever form cannot remedy the existing asymmetry. The consequence is that a solution in the existing body of consumer law must tackle the structural side, the digital architecture, by means

---

164 BVerfGE 89, 214 Bürgschaftsverträge (not officially translated by the GCC) (59). The GCC criticises in harsh words the reasoning of the Federal Supreme Court in civil matters: "For civil courts, this implies the obligation to ensure, when interpreting and applying general clauses, that contracts do not serve as a means of foreign determination. If the contracting parties have agreed on a regulation that is in itself permissible, further control of the contents will not be possible on a regular basis. However, if the content of the contract is unusually burdensome for one side and manifestly inappropriate as a balance of interests, the courts must not be content with the statement that 'a contract is a contract'. On the contrary, they must clarify whether the rules are a consequence of structurally unequal bargaining power and, where appropriate, take corrective action within the framework of the general clauses of the applicable civil law. How they have to deal with this and what result they must achieve is first and foremost a question of simple law, to which the Constitution leaves a wide margin of manoeuvre. However, a violation of the fundamental guarantee of private autonomy can be considered if we do not see the problem of disturbed contractual parity at all or if we try to solve it by inappropriate means.' https://www.servat.unibe.ch/dfr/bv089214.html

165 O. Ben-Shahar, C.E. Schneider, More than You Wanted to Know, The Failure of Mandatory Disclosure, Princeton, 2014.

166 (Ben-Shahar 2009); For a stock taking with regard to the EU (Micklitz, Sibony, and Esposito 2018),

other than information. That is why mobilising the prohibition on misleading actions and misleading omissions to fight digital asymmetry in the form of data exploitation strategies leads to a dead-end street.

4. *Scope of the UCPD*

(119) The UCPD has been adopted based on Article 114 TFEU. The Directive is therefore tied to the rationality of the internal market. Digitalization reaches beyond the market; it affects society. Does the EU have the competence to transform our societies?[167]

a) Protecting societal interests?

(120) There is overall agreement between those who critically analyse digitalization that its impact cannot be reduced to the economy. Most of the empirical debate is focusing on data collection and data processing strategies through which suppliers of digital services are enabled to affect consumer behaviour beyond mere economic transactions.[168]

(121) Are data exploitation strategies which reach beyond the market covered by the UPCD? Article 1 reads:

> The purpose of this Directive is to contribute to the proper functioning of the internal market and achieve a high level of consumer protection by approximating the laws, regulations and administrative provisions of the Member States on unfair commercial practices harming consumers' economic interests.

(122) The consumer has a role to play in the internal market. To carry out this task, they are provided with rights that they must exercise. This is the legacy of the Sutherland report and the deeper reason why the European Commission could successfully boost consumer law in the aftermath of the Single European Act. In order to open up the scope of application of Article 114 TFEU for secondary EU law, consumer concern had to be economised, reconstructed, and seen through the lenses of internal market rationality.[169] The struggle between Austria/Germany and the European Commission on how to deal with health claims is of paradigmatic importance. The jurisprudential debate between the legislature, the courts, and legal scholarship is characterised by different assessments of the role and function of the internal market.[170]

(123) Until now, the policy fields that the CJEU has been ready to exempt from the scope of application of the UCPD are small, and they deal with rather peculiar conflicts. The judgment

---

167 (Davies 2013, 53–70; 2015b; 2015a, 259–76)

168 (Natali Helberger 2020; Staahb 2019; Calo 2013)

169 (Bartl 2015, 572–98)

170 C-339/15 Vanderborght ECLI:EU:C:2017:335; C-356/16 Wamo und Van Mol ECLI:EU:C:2017:809

in *RLvS*[171] is much too specific to draw more general conclusions on whether or not the press activities of social media lie within or beyond the scope of application of the UCPD.[172] The consumer has a different role to play in the EU than in an orderly state system. The European Commission has recognised the difference through the concept of the *consumer citizen***,** subject to controversy in scholarship. On the one hand are those who fear marketisation of citizenship, on the other those who identify opportunities for civil action beyond the market.[173]

(124) In light of the order of competences the question is: whose task is it to regulate the overarching societal dimension of digitalisation – for the EU under Article 114 TFEU, or for the Member States? The competence creep of the EU, promoted and legitimized by the Court of Justice, has been discussed predominantly with regard to the backpacking of social and environmental policies in order to complete the internal market.[174] Full harmonization is taking away the power from the Member States to adopt higher standards or to deviate from the European legal framework in consumer and environmental law. The broader the scope of EU law, the narrower the notion of 'public interests', to which recital (5) UCPD refers as one of the possible escape roads for the Member States to step out of the scope of application. That is why any attempt to conceptualise misinformation solely as an economic construct sets the societal implications aside.

(125) Similar arguments apply to the exemption of '*culture*'. The UCPD does not deal with differences in culture.[175] Recital (7) refers to doorstep selling as an element of culture, which goes back to resistance by the new Member States against this form of sales promotion. The recital opens the door for a broad understanding of culture. Culture is about to lose its contours due to its ubiquitous use as a by-word far beyond law and *legal* culture. One might accept the idea of data privacy cultures, which differ between Europe and the United States,[176] but can we speak about 'differences in marketing culture' or 'differences in data privacy culture' so as to defend a particular national understanding of how commercial practices and data exploitation strategies should be used in the digital economy? Culture, if not given a rather narrow understanding, would and could lead to all forms of national economic protectionism, where culture serves as a placeholder for all sorts of entrepreneurial interests. It would re-introduce a kind of reasoning that the Court of Justice

171 CJEU Case C-391/12 RLvS ECLI:EU:C:2013:669 exempting newspaper publishers from the scope of application.

172 ECJ 9.11.2010 – C-540/08, ECLI:EU:C:2010:660 – Mediaprint Zeitungs- und Zeitschriftenverlag

173 (M. Everson 1995, 73–90; Michelle Everson and Joerges 2006) emphasizing the opportunities (Nic Shuibhne 2010, 1597–1628)

174 (Weatherill 2004)

175 Wilhelsson chapter 3 in (Howells, Micklitz, and Wilhelmsson 2006), pp. 58 same author, Osgoode Law Journal in which he identifies different cultural pconcatterns that need to be preserved despite full harmonization, (Wilhelmsson 2006)

176 (James Q Whitman 2004)

and later the EU legislature tried to abolish through the rationality test applied by the CJEU and through the Directives on unfair (2005/29) and misleading commercial practices (2006/114) which translated the case law of the CJEU into a binding EU regulatory framework. The reference to culture seems a double-edged sword, not to forget that the CJEU has given culture a rather narrow understanding in a very limited number of cases.[177]

(126) There is no other way than addressing the overarching effects of digitisation upfront. Online trade might serve as an example from the past to document what is at stake. Strong promotion of online trade through adoption of the Distance Selling Directive 97/7/EC and the E-Commerce Directive 2001/31/EC has operated to the detriment of local business in the cities. The EU has *de facto* manifestly changed our societies. This is not necessarily to our detriment, as Covid-19 has demonstrated. However, did the EU ever have the competence? True, the EU and the Member States operate in tandem. One-sided promotion of online business found support in most of the Member States. The responsibility is a joint one, though. Member States have played nested games.[178] Would the cities look different if Member States had to decide for themselves? Probably not.

b) Society and the EU Treaties

(127) The principle of enumerated powers offers *ex post* correction mechanisms at the national level and – as we will see – at EU level. At the national level, Member States may argue that commercial practices are beyond the scope of the UCPD when they interfere with politics and society. The standard formula of 'this needs to be decided case by case' is not satisfactory. The search for a conceptual answer goes deep as it requires a study of the degree to which the changes that the digital economy triggers are so fundamental that the constitutional architecture of the EU is affected. If the question is answered in the affirmative, the Member States would have to get together to discuss the foundations of European integration, how far market integration reaches, where society building starts and who should be competent for what. A less challenging way would be to activate Articles 114 (5) and 169 TFEU, which provide potential for the Member States and the EU to take action.

(128) Article 114 (5) TFEU, so far a mere fig leaf, could be turned into a powerful tool. It reads:

> if, after the adoption of a harmonisation …a Member State deems it necessary to introduce national provisions based on new scientific evidence relating to the protection of the environment or the working environment on grounds of a problem specific to that Member State arising after the adoption of the harmonisation measure, it shall notify the Commission of the envisaged provisions as well as the grounds for introducing them.

---

177 ECJ Case C-220/98 *Lifting* 2000 ECR I-117

178 (Tsebelis 1990)

(129) Good reasons can be advanced to argue that when the UCPD was adopted in 2005 nobody even thought of the digital economy and society. There are many legal barriers to overcome. New scientific evidence has been highlighted in the analysis of digital vulnerability under section 1. Article 114 (5) TFEU, however, seems to be based on evidence in natural sciences as the reference to the 'protection of the environment' makes clear. The 'working environment' could be a better reference point but would have to be given a broad understanding. Here the worker citizen ties in as counterpart to the consumer citizen. The highest barrier, though, is enshrined in the formula of 'a problem specific to that Member State'. Digitization of the economy and society affects all countries in Europe and around the world. In order to make a problem specific to that Member State, an additional parameter is needed. Here we are back to differences in 'culture', or even more sensitive, to 'national identity'. Poland for instance is defending the stationery business through legislative measures that conflict with EU law.

(130) But is it convincing to argue that data exploitation strategies belong to 'national identity'? There might be some room to argue that the existence of a national private law order belongs to national identity,[179] but it is a long way down from the private order to marketing practices or data exploitation strategies. The stakes for constitutional safeguards in the Treaty to protect the European legal order against national stand-alone actions are high, in particular when it comes to measures that bear a protectionist connotation, which is always the case when national regulatory measures end up in some sort of 'economic discrimination'.

(131) Article 169 (2) lit. b) TFEU enables the EU to take *minimum* 'measures which support, supplement and monitor the policy pursued by the Member States.' Article 169 (1) refers to promotion of 'the interests of consumers' and 'a high level of consumer protection', to 'protecting the health, safety and economic interests of consumers, as well as to promoting their right to information, education and to organise themselves in order to safeguard their interests'. The scope is somewhat broader than Article 114 TFEU, although the emphasis still seems to lie on the internal market. Integrating the societal dimension with 'economic interests' would enlarge the competences of the EU, though with one important difference: Regulatory measures dealing with the societal implications of the digital economy would be reduced to minimum harmonization.[180] Whichever way one might twist and turn it, EU law does not cover the societal implications of the digital economy, and even if it did so, defining the scope of application beyond the internal market would require political action and could not be left to the European judiciary alone.

---

179 (Micklitz 2011, 528–46)

180 (Reich, 2005, 383-407)

c) A preliminary reference as a game changer?

(132) The broad definition of commercial activities in the UCPD allows for measuring data exploitation strategies against the legal standards of unfair, misleading, and aggressive advertising and sales promotion. So far there has been little doubt, considering the CJEU judgment on the Data Privacy Directive 95/46/EC, the predecessor of the GDPR.[181]

(133) In May 2020 the German Federal Supreme Court referred a preliminary question to the CJEU, which, if answered in the affirmative, could potentially exclude data exploitation strategies from the UCPD. The litigation concerns a ruling which has been introduced into German law in the implementation of the GDPR. It grants legal standing to associations, including consumer organisations. Enshrined in the conflict is the question of the relationship between the UCPD and the GDPR, which is extensively debated in Germany and other Member States. Interested business circles had initiated a variety of litigation even before adoption of the GDPR on whether the law on unfair commercial practices could also deal with possible infringements of data privacy policies. In the litigation before the German courts, Facebook has built a similar line of argument so as to justify the primacy of the GDPR not only over competition law but also over the German Constitution.[182] The full harmonisation approach of the GDPR offered a new opportunity to seek confirmation for such a restrictive understanding before the CJEU. Interested parties claim that the GDPR conclusively regulates the rights of data subjects and that there is no room for consumer organisations to simultaneously attack possible infringements under the UCPD, a position which is backed by Article 3 (4) UCPD.[183] On the other end of the legal spectrum, leading voices point to the complementary character of the two sets of rules.[184] The preliminary reference concerns only the procedural dimension, namely the introduction of an action for injunction as an additional instrument of enforcing the GDPR without there being an infringement of individual rights. However, implicitly and behind the reference lies the much deeper and much more problematic question on the material scope of the GDPR and its relation to the UCPD. Here is the reference in full:[185]

> The Bundesgerichtshof stayed proceedings and referred a question to the Court of Justice of the European Union for a preliminary ruling on whether the rules laid down in Chapter VIII, in particular in Article 80(1) and (2) and Article 84(2) and (3), Regulation (EU) 2016/679 (the Basic Data Protection Regulation) preclude national rules which, in addition to the powers of

---

181 CJEU 29. July 2019 Case C-40/17, ECLI:EU:C:2019:629

182 As presented in discussion by the German Federal Supreme Court in its Beschluss KVR 69/19 23.6.2020.

183 (Philip Hacker 2020), provides for an account of the German debate under Ii) Taking Privacy and the GDPR into account, Fn. 81.

184 (Philip Hacker 2020; N. Helberger, Zuiderveen Borgesius, and Reyna 2017, 1439–43; Costa-Cabral and Lynskey 2017; Hacker 2018; Clifford, Graef, and Valcke 2019)

185 Beschluss vom 28. Mai 2020 - I ZR 186/17, see press release.

intervention of the supervisory authorities responsible for monitoring and enforcing the Regulation and the legal remedies available to the data subjects, grant competitors on the one hand and associations, institutions and chambers entitled under national law on the other hand the power to bring an action against the infringer before the civil courts for breaches of the General Data Protection Regulation, irrespective of the infringement of specific rights of individual data subjects and without any mandate from a data subject. This question is controversial in the case law of the courts of first instance and in the legal literature. It is argued that the General Data Protection Regulation contains a conclusive provision for the enforcement of the data protection provisions laid down in that regulation and that associations are therefore entitled to bring an action only under the conditions laid down in Article 80 of the General Data Protection Regulation, which have not been fulfilled in the case in dispute. Others do not consider the provisions of the basic data protection regulation on enforcement to be exhaustive and associations therefore continue to have the power to enforce injunctive relief for breaches of data protection provisions, irrespective of the breach of specific rights of individual data subjects and without a mandate from a data subject, by bringing an action before the civil courts. The Court of Justice of the European Union has already ruled that the provisions of Directive 95/46/EC (Data Protection Directive), which applied until the entry into force of the basic data protection regulation on 25 May 2018, do not preclude associations from having the right to bring an action (judgment of 29 July 2019 - C-40/17). However, it is not clear from that decision whether that right of action continues to exist under the basic regulation on data protection which replaces the Data Protection Directive.

(134) One has to recall that consumer organisations and trade organisations are in charge of surveying and monitoring advertising and marketing practices. Unlike in other Member States, neither Germany nor Austria has vested public authorities with related competences. As the Omnibus Directive (EU) 2019/2161[186] introduces remedies to the benefit of individual consumers that are harmed by unfair commercial practices, the judgment of the CJEU will also affect individual consumers and theoretically also those data privacy policies which are integrated into standard terms. If the CJEU answers the preliminary reference in the affirmative, opponents might stretch the argument and challenge the legal standing of consumer associations and consumer agencies to seek judicial review of data privacy policies as far as they are presented through standard terms.

(135) Centralizing the substantive and procedural rules of data privacy policies in one single legal document – the GDPR – would imply the inapplicability of other overlapping consumer protection rules that are apt to get to grips with unlawful data privacy policies. Consumers, consumer organisations, and consumer agencies would be deprived of the most powerful instruments they have been granted by Directives 93/13 and 2005/29. The action for injunction has been celebrated as the Europe-wide minimum standard of collective redress.

186 Poland belongs to those Member States which had interpreted the former Art. 11 (2) Directive 2005/29 to introduce the obligation to grant standing to individual consumers. In that sense the Omnibus Trade Directive is nothing more than a confirmation. I would like to thank Monika Namyslowska for this information.

The remedy allows co-ordination of regulatory actions across Europe, which has turned into a much more powerful tool than transborder litigation.[187] Especially in light of digital asymmetries, co-ordinated actions are a means of exercising countervailing powers. Provided the CJEU is ready to follow the 'imperialistic understanding of full harmonization', Member States are called upon not only to initiate a serious debate on full harmonization but also to take regulatory countermeasures. The Directive on representative action is meant to put an end to the debate. The GDPR is added to Annex II, the list of Directives which come under Article 7 (5) UCPD.[188]

5. *A common approach on fairness under the GDPR, UCPD and UCTD*

(136) Further analysis starts from the premise that data exploitation strategies could and should be regarded as commercial practices and that the scope of application of the UCPD remains open, above and beyond the GDPR. A holistic perspective requires inclusion in the analysis of data exploitation policies which are enshrined in standard terms and can therefore be submitted to judicial control under the UCTD. The three legislative measures, though different in scope and reach, are claimed to be based on a common denominator that underpins the measures but that does not fully exhaust policy objectives, which might differ in detail: the argument is that the three measures are meant to ensure that consumers are treated fairly, as subjects of privacy concerns, as addressees of commercial practices, or as contracting partners. Thereby the EU is institutionalising market fairness, but only if a common benchmark cuts across the different legislative elements

a) The control architecture

(137) As a starting point, one may want to recall the legal definitions which the three legislative measures prescribe and that not only define the scope but also lay the ground for the control architecture:

> GDPR Article 2 (1):This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
>
> UCPD Article 2 (1): For the purpose of this directive (d) 'business-to-consumer commercial practices' (hereinafter also referred to as commercial practices) means any act, omission, course of conduct or representation, commercial communication including advertising and

187 BEUC has initiated the new strategy, The Report of the Consumer Law Enforcement Forum CLEF and of the Consumer Justice Enforcement Foirmum COJEF, https://www.beuc.eu/general/consumer-justice-enforcement-forum-cojef

188 Annex I (56) Directive 2020/1828 on representative actions for the protection of the collective interests of consumers, and repeal ing Directive 2009/22/EC , p, OJ L 409/1, 4.12.2020.

marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers;

UCPD Article 11a (1): Consumers harmed by unfair commercial practices shall have access to proportionate and effective remedies, including compensation for damage suffered by the consumer and, where relevant, a price reduction or the termination of the contract. Member States may determine the conditions for the application and effects of those remedies. Member States may take into account, where appropriate, the gravity and nature of the unfair commercial practice, the damage suffered by the consumer and other relevant circumstances.

UCTD Article 3 (1): A contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer.

UCTD Article 3 (2): A term shall always be regarded as not individually negotiated where it has been drafted in advance and the consumer has therefore not been able to influence the substance of the term, particularly in the context of a pre-formulated standard contract.

(138) The purpose here is not to engage in a debate over how far the overlap reaches and which is the broader rule. Whilst this would certainly be a useful exercise, attention should be drawn to the legislative architecture of the fairness test, the interplay between standardised forms of data exploitation strategies and non-standardised policies, with which different forms of legal remedies can be associated, and last but not least how they are to be evaluated under the three distinct pieces of consumer law.

(139) In this perspective, the oldest Directive – 93/13/EEC – provides the most outspoken control architecture. The distinction is very well established although not free from critique.[189] Standardised terms are subject to judicial control independently of an individual infringement.

(140) A similar distinction now governs commercial practices. Commercial practices are by nature a form of standardised marketing strategy. That is why the enforcement of possible infringements is put into the hands of consumer agencies or consumer organisations, or both. Collective public or private enforcement is not connected to an actual infringement but, rather, the *likelihood* of a possible infringement suffices in principle to trigger the enforcement mechanism. The CJEU has held that even commercial practices that target one single consumer come under the scope of application,[190] and the Omnibus Directive has granted consumers the individual right to pursue. This means that the consumer who is targeted individually may enforce their rights individually and is no longer dependent on collective enforcement, whether private or public.

189 (Micklitz 2014), more comprehensively same author (Micklitz 2007, 387–410), reprinted in (Micklitz 2008, 19–42)

190 CJEU C-388/13 UPC Magyarország ECLI:EU:C:2015:225

(141) The GDPR addresses, for example, the processing of personal data by automated means. Automation implies standardisation, as there is no automation without standardisation. This is the input side. On the output side, there may be standardisation or personalisation. Data may be used to target consumers as such, a particular group of consumers, or consumers individually.[191] This means that the degree of personalisation varies according to the algorithm used to evaluate the collected data. On the enforcement side, the GDPR relies mainly on individual enforcement, which might be in line with the personal character of the data but which overlooks that data processing is a standardised exercise, which could be much better monitored and surveyed through collective enforcement. In contrast to the UCTD and the UCPD, the GDPR has not introduced legal standing for consumer agencies or consumer organisations. This lacuna has been remedied through Directive 2020/1818 on Representative Actions.

(142) The control architecture can be broken down into a two-layer structure, in the shape of standardisation – which in principle is abstract and general – and individualisation, which refers to concrete circumstances.

	UCTD	UCPD	GDPR
Standardised Abstract general	Standard terms + collective enforcement (public/private)	Standardised commercial practices + collective enforcement (public/private)	Automated (standardised data processing) + individual collective enforcement (public/private)
Individualised Concrete individual	Individually negotiated terms + Individual enforcement	Individualised commercial practices + individual enforcement	Individual rights to information and explanation

(143) In *Pereničová and Perenič*, AG Trstenjak laid down rules on the interaction between the UCPD and the UCTD. The CJEU had to draw the boundaries between commercial practices and contract terms. Following AG Trstenjak, the Court held that a contracting practice violating the UCPD does not automatically count as unfair under the unfair contractual terms directive (UCTD).[192] However, provided the contracting practice is to be regarded as an unfair commercial practice, this assessment must be considered as one of the elements in the

191 On standardisation, personalisation and individualisation, see Area 2 H.-W. Micklitz/P. Rott, Personalised Prices and Personalised Marketing, BEUC Study 2020.

192 AG Trstenjak, Opinion, Case C-453/10, Pereničová and Perenič , ECLI:EU:C:2011:788, para. 89-90, Case C-453/10, Pereničová and Perenič , ECLI:EU:C:2012:144, para. 43-44; Case C-109/17, Bankia ECLI:EU:C:2018:735, para. 49, Keirsbilck, Bert. "Interaction between Consumer Protection Rules on Unfair Contract Terms and Unfair Commercial Practices: Perenicova and Perenic." Common Market L. Rev. 50 (2013): 247.

fairness test under the UCTD. German courts treat a breach of unfair contract terms law at the same time as a breach of unfair commercial practices law.[193]

(144) UCPD unfairness cannot be neglected when assessing the fairness of data exploitation strategies under the GDPR. Therefore, the *Pereničová and Perenič* doctrine is equally applicable with regard to interaction between the GDPR and the UDPD.[194] The rule applies both ways, at least as long as the specificities of the respective field of regulation are set aside. The overall purpose should be to seek a common denominator between the various fairness tests to avoid inconsistent value judgments. The working hypothesis is that data exploitation strategies should be understood as infringing fairness under all three fields of law.

(145) However, the lessons to learn reach beyond substance. The case law of the CJEU on the UCTD provides guidance on the linkage between the standardised and the individual levels, on the binding effect of judgments taken at the abstract level on the concrete level, and last but not least on the role of courts in evaluating fairness. In a whole series of judgments, the CJEU has insisted that the consumer must have the opportunity to provide *ex post factum* consent to standard terms that are not in compliance with EU law. The unlawfulness of standardized terms is therefore no more than a presumption which the consumer may invoke in an individual case or not.[195] Therefore consent may in theory legitimate the blameworthy abstract unfairness of the standard term – provided the consumer knows and understands what they are consenting to in their individual litigation. It will have to be shown that consent can only justify abstract unfairness if a whole series of safeguard measures are established so as to guarantee consumer autonomy.

(146) The extension of *res judicata* engaged the CJEU in *Invitel*,[196] without, however providing clear guidance on whether the Member States are obliged under EU law to give *erga omnes* effect to actions for injunctions declaring a contract term to be unfair.[197] The new Directive on Representative Actions does not provide for such an effect, although this had been discussed intensely in the evaluation of the Injunctions Directive 2009/22/EC. In contrast, the CJEU has not only recognized but also gradually extended the so-called *ex officio* rule: the obligation of the competent court to investigate *ex officio* whether a contract terms infringes the UCTD.[198] The reach and potential function of the *ex officio* rule will be tested in terms of what

193 See BGH NJW 2012, 3577, 3580 f.

194 In this sense (Philip Hacker 2020)

195 C. Leone, (2020). The missing stone in the Cathedral: Of unfair terms in employment contracts and coexisting rationalities in European contract law.

196 ECJ C-472/10 Invitel, 2012, ECR I ECLI:EU:C:2012:242

197 (Micklitz 2014) and more comprehensively, H.-W. Micklitz/N. Reich, Von der Klausel- zur Mißbrauchskontrolle EuZW 2013, 457.

198 (Beka 2018)

national courts should be doing *in concreto* when confronted with the technological settings – the ground level of data exploitation policies.

b) Control architecture, data exploitation strategies, and commercial practices

(147) In contrast to the UCPD and the UCTD, the GDPR is not built around what is forbidden and what kind of marketing strategies and contract making are to be avoided. Quite to the contrary: the philosophy behind the GDPR is to lay down the requirements that the 'processor' (Article 4 (8)) has to respect, i.e. the rules the processor should respect in order to comply with the law. This does not mean that the GDPR does not define thresholds for collecting and recording data. However, these few requirements do not change the overall regulatory structure. The GDPR does not use the language and concepts established in EU economic law, such as supplier, customer and consumer, despite the overall objective of the GDPR to establish a regulatory framework for 'the free flow of personal data in the Internal Market', according to Article 1 (3) GDPR. Sections 1 and 2 stress the money-making side of data processing, the business strategies applied so as to use the free flow of personal data for profit-seeking purposes. There is a mismatch between the regulatory philosophy, the language, and the concepts, a mismatch that insinuates a kind of neutrality on the part of the GDPR and the foundational role and function the GDPR plays for the governance of economic transactions. [199]

(148) Browsing through the 88 pages of the law discloses that the word 'commercial' is referred to four times. Article 57 (1) i) is the single reference point which builds a bridge to commercial strategies: 'The supervisory authorities are required to monitor relevant documents, in particular the development of information and communication technologies and *commercial* practices'. This reference is all the more amazing as the supervisory authorities, being in charge of controlling the application of the GDPR, are also competent to dive into a different legal world, namely the law on unfair commercial practices and the law on unfair standard terms. At least this is what the wording suggests. The GDPR does not clarify what is meant by commercial practices, whether it is used in the meaning given to this term in Directive 2005/29/EC or whether it also covers standard terms which are equally to be regarded as a form of commercial practice. One has to look elsewhere in order to find guidance on the business side of data processing as defined in Article 4 (2). Quite common in the business environment but also in European Economic and European Consumer Law is the rather broad language of 'data privacy policies'.

(149) *Techopedia* for instance gives the following definition:[200]

---

199 (Micklitz, 2020).

200 ("What Is Data Protection Policy? - Definition from Techopedia" 2017)

> A data protection policy is a type of security policy that aims to design, implement, guide, monitor and manage security over an organization's data. It primarily aims at securing and protecting logical data stored, consumed, and managed by an organization. This data can be stored within the organization core infrastructure, offsite location or at an online / cloud service.

(150) More telling and helpful might be the following explanation:

> The key objective behind a data protection policy is ensuring the security and integrity of data at rest and in motion – regardless of its physical or logical location. A data protection policy will be designed to ensure security across all the data storage / consuming location.

(151) A comprehensive data protection policy includes: Scope of data protection, data protection method/ policy at the granular level i.e. individual, department, device and/or IT environment, **legal requirements for data protection,** roles and responsibilities of data custodian or staff that will ensure data protection (emphasis added).

(152) Data privacy policy reaches beyond pure compliance with legal requirements, under which companies are allowed to lawfully collect data from consumers, either via prior consent or via being able to invoke legitimate reasons why collection of data is needed. It comes close to the terminology used in section 3 on data exploitation strategies. However, data exploitation is more concise in a twofold sense: it commercializes the rather neutral language of data processing and data policy and emphasises the fact that there is a business plan, a commercial strategy, behind the data collection. Data exploitation can in principle be submitted under the definition of 'commercial practices' in the UCPD and under 'standard terms' in the UCTD, depending on the surface level of how the data exploitation strategy is communicated to the consumer. This is the established view of the German courts.[201]

(153) This is equally true of the CJEU. Right from the first cases to be decided under Directive 2005/29/EC, the CJEU defended a broad definition. Commercial practices in Article 2 (1) UDCPD are understood as 'communication', which 'includes' information-based advertising and non-information-based sales promotion before, during and after conclusion of a contract.[202] Data exploitation strategies typically precede economic transactions, regardless of whether they are formalised in a contract or whether they remain unformalized but nevertheless legally relevant.[203] The *ex post* effects of data exploitation strategies are of utmost relevance. Their true impact might lie in the post contractual phase, as personal data are collected for all sorts of possible uses that not even the supplier will know in advance. It

---

201 See LG Berlin, 19/11/2013, *MultiMedia und Recht* 2014, 563, at 565 – *Google*; LG Berlin, 30/4/2013, *Neue Juristische Wochenschrift* 2013, 2605, at 2606 – *Apple*; LG Frankfurt a.M., 10/6/2016, *Beck Rechtsprechung* (BeckRS) 2016, 10907 – *Samsung*. See also (Rott 2017).

202 C-476/14 *Citroën Commerce* ECLI:EU:C:2016:527 at 43 'during and after the contract' under reference to Abcur, C-544/13 and C-545/13, EU:C:2015:481, at 73

203 (Palka, 2018)

is highly debatable whether the purpose specification and the data limitation principles suffice to monitor and survey the post contractual phase.

(154) Most of the phenomena that characterise external-structural digital asymmetry could be qualified as technological infrastructure which is developed and installed prior to contacting the consumer. The UCPD as amended by the Omnibus Directive (EU) 2019/2161, to be implemented by 31.12.2021, refers in Article 2 c) to digital services and – in the newly introduced Article 2 m) and n) to rankings and online market places. However, technological infrastructure is not explicitly mentioned. That is why the solution must be found in the definition of the scope of the Directive.

(155) Analysing data exploitation strategies in light of the broader legal architecture, one feels reminded of contract law, where business and/or business organisations elaborate standard terms prior to conclusion of a contract, so as to impose them on consumers, whose only choice is between 'take it or leave it'. Negotiations on pre-formulated standard terms are the exception to the rule and if consumers try their claims are often rejected. That is why Article 3 (3) of Directive 93/13/EEC has shifted the burden of proof for the existence of pre-formulated contract terms to the supplier. This kind of reasoning can be transferred to data exploitation strategies. Rationalisation serves as the standard argument to justify and to legitimate pre-formulation for a particular business or even for a whole industry. Data exploitation strategies pursue precisely this objective. Providers are neither willing nor able to negotiate with the consumer individually as to which data should be collected for what purposes. Pre-formulated options do not undermine the standardising character. The options offered are equally pre-designed and pre-formulated. They form an integral part of the technological infrastructure and should not be understood as a form of negotiation. In Germany, consumer organisations have successfully brought to court companies that started to use different default settings in standard terms to insinuate individuality.[204] So far the CJEU has not had to deal with default settings in data exploitation strategies as a form of commercial practice. However, the CJEU confirmed that default settings are covered by the Directive.[205] If, and if so under what conditions, data exploitation strategies allow for a reversal of the burden of proof remains to be discussed below. In *Planet 49* the CJEU held that pre-ticketing does not constitute valid consent within the meaning of Articles 5(3) and 2(f) of Directive [2002/58], read in conjunction with Article 2(h) of Directive [95/46].[206]

---

204 F. Bultmann, 30 Jahre Praxis der AGB-Verbandsklage, Gutachen im Auftrag der Verbraucherzentrale Bundesverband, 2008 with references to the judgments of the Federal German Supreme Court, pp. 47 https://www.vzbv.de/sites/default/files/downloads/gutachten_30_jahre_verbandsklage_vzbv_2008.pdf

205 C-611/14 *Canal Digital Danmark* ECLI:EU:C:2016:800; C-310/15 *Deroo-Blanquart* ECLI:EU:C:2016:633; Combined cases C-54/17 and C-55/17 *Wind Tre* ECLI:EU:C:2018:710

206 CJEU Case C-673/1z ECLI:EU:C:2019:801 and the follow-on judgment of the German Supreme Court, I ZR 7/2016.

(156) Qualification of data exploitation strategies as commercial practices has far reaching implications for the exercise of control parameters. **Data exploitation strategies should be understood as sales promotion measures, which are traditionally regarded as a counterpart to information-based advertising.** Data exploitation strategies set up a structure which remains external to the consumer. This has been amply demonstrated in the analysis of digital vulnerability. That is why the asymmetry which data exploitation strategies establish cannot be overcome through information techniques. Thus, the decision whether they are lawful or not cannot be based on the information paradigm, which governs assessment of misleading advertising. Sales promotion techniques prevail over sediments of information. In a whole series of judgments, the CJEU interpreted sales promotion technique as being covered by the Directive.[207]

c) Sequence of the legality check

(157) Qualifying data exploitation strategies as commercial practices affects the way in which order the rules of the UCPD must be examined. The UCPD must be understood as a reverse pyramid: on top are the blacklisted practices in the annex, then the specific general clauses – the prohibition of aggressive commercial practices of Articles 8 and 9 and the prohibition of misleading actions and misleading omissions of Articles 6 and Article 7– and last but not least the safety net enshrined in the general unfairness test under Article 5 UCPD. Data exploitation strategies might qualify as aggressive commercial practices, but their legality will also have to be examined against the professional diligence requirement.

(158) Analysis under whatever legal regime has to duly consider that data exploitation strategies could only be regarded as *per se* unlawful if they had been prohibited as blacklisted practices. But even here the CJEU is not given adjudicatory power to decide 'the case'. It is for the CJEU to interpret the Directive and for the Member State courts to apply the guidance provided by the CJEU to the facts. The contradiction between the design of legal regimes on commercial practices and on standard terms is documented in a long standing list of examples where the CJEU decided the case *de facto* through extensive guidance which left no choice for the national court.[208]

(159) The distinction between legal analysis under EU law and the facts that have to be added in order to justify the qualification as unlawful poses particular problems in terms of assessing data exploitation strategies as potentially unfair commercial practices. As the law stands, more is needed than mere data exploitation strategies. They must include an element of unfairness which is peculiar to that particular strategy. However, lack of knowledge of

---

207 *ECJ* 23.4.2009 – C-261/07 und C-299/07, ECLI:EU:C:2009:244 – *VTB-VAB*, at 48*; ECJ* 4.1.2010 – C-304/08, ECLI:EU:C:2010:12 – *Plus Warenhandelsgesellschaft*, at. 35; *ECJ* 9.11.2010 – C-540/08, ECLI:EU:C:2010:660 – *Mediaprint Zeitungs- und Zeitschriftenverlag,* at 17. see Guidelines 2016, pp 13, 14.

208 (Micklitz and Reich 2014).

whether a data exploitation strategy contains such an additional element is inherent to digital asymmetry. Here the reversal of the burden of proof comes into play. In the following, we will demonstrate that data exploitation strategies should be regarded *prima facie* as *potentially* unfair aggressive practices and/or as *potentially* infringing professional diligence subject to proof of the contrary. It is for the user to provide evidence that they have taken the necessary safeguard measures to avoid infringing the law on unfair commercial practices.

6. *Aggressive practices*

a) Blacklisted aggressive practices

(160) All blacklisted practices which are built in one way or the other on misleading information – through action or through omission – can be set aside for the purposes of this study. What remains are blacklisted aggressive practices. Out of the eight practices listed in Annex I to the UCPD none comes even close to the phenomenon of external structural digital asymmetries enshrined in the concept of digital exploitation strategies. A couple of judgments on no. 29 deal with unsolicited goods and services[209] and on no. 31 with sweepstakes.[210] They do not allow drawing more general conclusions either on the scope or on the understanding of aggressive commercial practices. The fact that the UCPD did not introduce a mechanism for adoption of blacklisting changes through a comitology procedure may have its revenge.

(161) The amendments to no. 11 a) and no. 23 a-c) by the Omnibus Directive deal with forms of misleading commercial practices. This is particularly striking as the Directive was adopted after the GDPR at a time when problems stemming from unfair data exploitation strategies were already obvious.

b) Aggressive practices before the Court

> Article 8 UCPD: A commercial practice shall be regarded as aggressive if, in its factual context, taking account of all its features and circumstances, by harassment, coercion, including the use of physical force, or undue influence, it significantly impairs or is likely to significantly impair the average consumer's freedom of choice or conduct with regard to the product and thereby causes him or is likely to cause him to take a transactional decision that he would not have taken otherwise.

---

209 Combined cases C-54/17 und C-55/17 *Wind Tre* ECLI:EU:C:2018:710, Rs. C-406/17 bis C-408/17 und C-417/17 *Acea Energia* ECLI:EU:C:2019:404

210 C-428/11 *Purely Creative u.a.* ECLI:EU:C:2012:651

> Article 9 UCPD: In determining whether a commercial practice uses harassment, coercion, including the use of physical force, or undue influence, account shall be taken of: (a) its timing, location, nature or persistence; c) the exploitation by the trader of any specific misfortune or circumstance of such gravity as to impair the consumer's judgement, of which the trader is aware, to influence the consumer's decision with regard to the product;
>
> Article 2 j) UCPD: For the purpose of this Directive: 'undue influence' means exploiting a position of power in relation to the consumer so as to apply pressure, even without using or threatening to use physical force, in a way which significantly limits the consumer's ability to make an informed decision;

(162) The concept of aggressive commercial practices had been unknown to the legal orders of the Member States. The Directive broke new ground which, however, is just about to come before the CJEU. Neither the Directive nor the recitals or the Guidelines of the European Commission[211] provide useful guidance on how 'aggression' should be understood as an umbrella concept for harassment, coercion and undue influence. Every form of advertising contains an element of aggression, which is socially tolerated in a market economy. However, when does aggression cross the red line and become no longer acceptable and therefore illegal? Can data exploitation strategies be qualified as aggression?[212]

(163) Out of the three listed forms, undue influence is the one that should receive a prominent position in control of data exploitation strategies. It is also the only one which shows similarities to existing rules in the Member States. Here, Article 2 j) gives a definition. A first reading seems to confirm that Article 8 in combination with Article 2 j) is best suited to test the legality of data exploitation strategies.

(164) Here is where the Court stands today: In two recent judgments in the cases of *Wind Tre*[213] and *Orange Polska*[214] the CJEU for the first time had the opportunity to concretise the requirements to qualify commercial practices as aggressive through the exercise of undue influence. In both cases Advocate General Campos Sanchez-Bordona wrote the opinion. *Wind Tre* deals with default settings in the promotion of SIM Cards where the internet and mailbox service are already installed, without properly informing the consumer of that fact and the potential costs. *Orange Polska* turned on the marketing of telecommunication contracts where the consumer had to take the final decision on whether they wanted to

---

211 COMMISSION STAFF WORKING DOCUMENT GUIDANCE ON THE IMPLEMENTATION/APPLICATION OF DIRECTIVE 2005/29/EC ON UNFAIR COMMERCIAL PRACTICES Accompanying the document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses, SWD/2016/0163 final.

212 For more details Part 1.

213 CJEU C-54/17 *Wind Tre* ECLI:EU:C:2018:710.

214 CJEU C-628/17 *Orange Polska* ECLI:EU:C:2019:480

conclude a contract or not under the physical presence of the courier who handed the contract out.

(165) The CJEU's line of argument runs like this: Contrary to blacklisted practices, commercial practices which come under the scope of Articles 8 and 9 can never be unlawful as such. Recital (17) of Directive 2005/29/EC specifies that, in order to provide greater legal certainty, only the practices listed in Annex I are deemed unfair in all circumstances without having to be assessed on a case-by-case basis against the provisions of Articles 5 to 9 of that directive. According to the CJEU an aggressive practice has to affect both the consumer's freedom of choice and their freedom of conduct.

(166) Freedom of choice implies that the consumer has been properly informed. The yardstick is the average consumer, who, however, cannot be expected to have the necessary skills to change the default setting alone. The mere withholding of relevant information in *Wind Tre* or the physical presence of the courier in *Orange Polska* cannot be qualified as aggressive as such. Undue influence, so goes the rationale of the judgment, requires a situational action which must not be unlawful but which must be apt to put undue pressure on the consumer's freedom of choice and conduct. The CJEU requires 'additional practices'. The German version of the judgment translates additional practices, misleadingly, as 'unlautere Verhaltensweisen', i.e. to unfair practices.[215] In *Orange Polska*, the Court provides guidance of what these additional practices might be, for example time pressure from the courier. In *Wind Tre*, the CJEU based its judgment against the opinion of the Advocate General on the per se prohibition of no. 29 of Annex I, thereby avoiding discussion on the scope and meaning of aggressive practices in Articles 8 and 9. Additional measures are said to constitute an aggressive practice if they are 'liable to make that consumer feel uncomfortable and thus to confuse his thinking in relation to the transaction decision to be taken'.[216]

(167) Four uncertainties are apparent in the CJEU's interpretation of aggressive commercial practices. *First*, in neither of the two decisions did the CJEU provide guidance towards understanding a 'position of power'. AG Sanchez-Bordona made a proposal, which the CJEU did not take up:[217]

> As I recalled in the Opinion in Wind Tre and Vodafone Italia, a distinction must be drawn between two aspects of the position of power - on the one hand, the exploitation of a position of power which allows the trader to infringe the consumer's freedom when it comes to buying a product; - on the other hand, the position of power held in law by a trader who, following the conclusion of the contract, may claim from the consumer the consideration which the latter undertook to provide on signing the contract.

---

215 Orange Polska at 46.

216 Orange Polska at 47.

217 Orange Polska at 47 .

(168) Legal scholarship proposes to reduce the power position to economic power as the Directive aims at protection of economic interests. This might be too narrow, as power can also be exercised intellectually or technologically,[218] so that power forms an integral part of digital vulnerability and therefore of digital asymmetry.

(169) *Secondly*, the CJEU puts emphasis on the key role of information even within examination of aggressive practices, and *thirdly*, the CJEU did not clarify under what circumstances a lack of information results in significant impairment. In *Orange Polska*, lack of information must affect the consumer's choice;[219] In *Wind Tre* the AG more or less reiterates the rather unclear wording of the Article.[220] *Fourthly*, perhaps even more difficult, is a criterion which the CJEU did not examine either in *Wind Tre* or in *Orange Polska*: Article 9 c) requires the authority or court to take into account that the trader '*must be aware*' rather than '*should be aware*' of the fact that exploitation by the trader of any specific misfortune or circumstance is of such gravity as to impair the consumer's judgment.[221]

c) Data exploitation strategies as aggressive practices

What does the case law give us in terms of assessing the lawfulness of data exploitation strategies? Both AG Campos Sanchez-Bordona and the CJEU insist on the key role of information in securing freedom of choice. Thereby the CJEU intermingles the two concepts – Articles 6 and 7 on misleading and missing information and aggressive practices in Articles 8 and 9. Considering the overall structure of the Directive, this intermingling is unacceptable. Articles 8 and 9 deal with forms of commercial practice that qualify as unlawful for reasons other than 'information deficit'. It seems far-fetched to assume, in light of the analysis of universal digital vulnerability, that more or better information can help the consumer to make a better decision. The consumer is locked in the institutional design of data exploitation strategies. There is no way out, and even if there were a way out, information is not the appropriate tool. One might argue that the CJEU uses the reference to Article 8 as an argument to strengthen the importance of misleading omissions under Article 7. The consequence would be to read deficits in the digital architecture that contradict the prohibition of misleading omissions. However, the dividing line between the two concepts – information-based commercial practices (often equated with advertising) and non-

218 (Micklitz and Namyslowska 2020a)

219 At 46

220 At 63. 'That outcome has to take the form of an impairment, actual or potential, to the consumer's freedom of choice with regard to the product so 'significant' as to give rise to or be likely to give rise to a decision which the consumer would not have taken otherwise. In accordance with that provision, that objective must have been achieved by 'harassment, coercion, including the use of physical force, or undue influence'

221 (Philip Hacker 2020), under reference to (Caronna 2018), who even demands intentionality, and with further references from German legal doctrine who support such interpretation.

information based commercial practices (often equated with sales promotion) – needs to be upheld.

(170) In light of this decisive distinction and in regard to the key role of 'undue influence' the question is whether external structural asymmetry inherent in data exploitation strategies could be regarded as a form of undue influence. The various forms of structural asymmetry – the digitally mediated relationship, the choice architecture, the architectural infrastructure, and the knowledge structure – combine two forms of power: economic power and intellectual power, which both lie in the hands of businesses. They 'influence' consumers' leeway for action and prevent them from making an 'informed decision', but not because the information is misleading, but case information is substituted through structural aggression. In *Wind Tre* the CJEU seemed inclined to accept that understanding in assuming that the consumer is not able to change the default settings. Articles 9 a) and c) may underpin the assumption that *structural* power comes under the scope of application of Article 9 as a particular form of 'undue influence'. Article 9 a) highlights the aspect of timing, which is crucial for assessing predefined data exploitation strategies. Article 9 c) refers to impairment of a consumer's capability in assessing the influence exercised on them.[222]

(171) But can there be *structural* influence and/or structural pressure? Does pressure presuppose that the consumer is aware of being pressured or the target of undue influence?[223] The wording of Article 9 c) seems to prevent the applicability of aggressive practices to structural phenomena. The supplier 'must be aware' of the pressure, of the influence it is exercising. Taken literally, the supplier must establish the data exploitation strategy *intentionally* so as to exercise pressure on the consumer. Through such an interpretation the law on unfair commercial practices is thrown back to its origins, to tort law, to negligence, and here even intention. This would make the prohibition of aggressive practices less than useful because the barriers are unsurmountable. In the business environment, most companies that use data exploitation strategies will not have developed them, but are using data exploitation strategies which are set up and monitored by the few companies around the world which apply to process large amounts of data. This immediately raises the question whether the companies using these externally developed data exploitation strategies are equally legally responsible. The counterargument against such a narrow understanding results from the wording of Article 8 which defines the basic rules for what should be understood as aggressive. In line with the overall regulatory philosophy behind the law on unfair commercial practices, Article 8 distinguishes between 'impair' and 'likely to impair' the average consumer's freedom of choice or conduct. Likelihood is sufficient for all sorts of aggressive practices. Article 9 c) in combination with Article 2 j) cannot set Article 8 aside.

222 (Micklitz and Namyslowska 2020b).

223 (Philip Hacker 2020), insists that awareness is required.

Articles 9 and 2 j) concretise Article 8. Finally, taking the wording in Articles 9 and Article 2 j) literally would bring Directive 2005/29/EC even closer to contract and tort law, which, however, will not be affected through European legislation. That is why Article 8 should be understood as covering the likely impact of structural digital asymmetry on the consumer.

(172) Let us assume, for the sake of argument – without looking at what remains for national courts – that data exploitation strategies are to be regarded as potentially unfair. Would such a prohibition set an end to commercial practices which aim at collecting data and processing them for purposes that the consumer cannot overlook and understand? The German Federal Supreme Court assessed the data privacy policy of Facebook in light of German competition law. The German court requires, provided it confirms its preliminary decision in the final judgment (which is highly likely), that Facebook has to offer the consumer a true choice between subscribing to the service with and without the use of personal data.[224] This would be a revolution in the digital economy. The German Advisory Board of Consumer Affairs advocated the possibility that suppliers disclose their technological infrastructure (the algorithms behind) to an as yet non-existent digital agency which would be in a position to assess them and their possible impact on data processing.[225]

7. Data exploitation strategies as infringement of professional diligence

(173) The debatable reach of Articles 8 and 9 makes it necessary to test whether data exploitation strategies could also be understood as an infringement of the general clause in Article 5 (2), and if so, what kind of requirements would have to be fulfilled. This would mean that data exploitation strategies are to be regarded as an infringement of professional diligence – as defined in Article 2 h): *'professional diligence' means the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity* – which 'materially distorts or is likely to materially distort the economic behaviour of the average consumer or of the average member of the group when the default setting is directed to a particular group of consumers'.

(174) Until now, the CJEU has not provided much guidance on concretizing the notion of professional diligence. Legal doctrine ventilates the possibility of imposing on suppliers the obligation to take precautionary measures through auditing so as to make sure that the technological infrastructure they apply in the processing of data complies with the law.[226]

---

224 (Palka 2021).

225 (Advisory Council of Consumer Affairs to the German Federal Ministry of Justice and Consumer Protection, n.d.)

226 (Philip Hacker 2020), p. 15 with references

This obligation goes along with the UCPD Guidelines of the European Commission.[227] Much less discussed are the legal consequences that result from the *ex post* effects of data exploitation strategies. The UCPD covers commercial practices in the post contractual phase. Findings in behavioural as well as in communication science underpin the crucial importance of the post-contractual phase. Connecting the scope of the UCPD to professional diligence opens new pathways for establishing post-contractual duties of care.[228]

(175) If precautionary measures and *ex post* duties of care do not exist, a material distortion or the likelihood of a material distortion is supposed to exist. One might wonder why such an examination cannot be exercised by the courts or by supervisory agencies. What is thinkable in theory fails in practice. Neither courts nor supervisory agencies have the necessary human and economic resources to test data exploitation strategies, more concretely to find out whether the algorithms which stand behind data exploitation strategies are designed so as to produce unlawful effects. The proposal to rely on auditors might therefore result much more from the non-existence of resources than from the impossibility of building up those resources.

(176) However, outsourcing the compliance test to an auditing company produces new problems, which are widely discussed regarding certification bodies. Auditing companies need to be accredited and their activities need to be controlled. The PIP breast implants saga documents that the regulatory framework on certification and accreditation in the field of medical devices is far from sufficient.[229] On top of this, auditing companies would need guidance on what exactly they have to search for. Professional diligence would have to be concretised to provide a benchmark for assessing the lawfulness of data exploitation strategies. This could be done in various ways. The regulatory approach of the UCPD points to blacklisted practices as a relatively simple yardstick of control. However, as it stands the list is of no help. New blacklisted practices would have to be introduced. The other – not necessarily mutually exclusive – option is to refer to a regime where business, supervisory authorities and consumer organisations co-design the necessary benchmarks.[230] To put it bluntly: what is needed is a shift from new approach type co-regulation to co-design of regulation.

(177) Delegation of the precautionary fairness test to an auditing company does not free the supplier and user of data exploitation strategies from its own responsibility. But who exactly is in breach if no such auditing exists or is done improperly? The user who is relying on externally developed data exploitation strategies might not be in a position to supervise,

---

227 Guidance European Commission, p. 126

228 Section 1 2.

229 (Rott 2019)

230 For discussion see (Advisory Council of Consumer Affairs to the German Federal Ministry of Justice and Consumer Protection, n.d.)

monitor and control the inherent technological infrastructure. Under the GDPR this kind of responsibility is in the hands of the data controller, according to Article 4 (7). The concept cannot easily be transferred to the UCPD. The user is usually not the developer of data exploitation strategies. It is not able to control the data, nor is its controller. Hacker[231] proposes holding the user responsible only if it 'controlled the breach' or 'should have known' about the breach. The insertion of negligence requirements, however, does not go along with the regulatory approach of the UCPD. Infringement does not require fault on the part of the wrongdoer. The question whether the user intentionally or negligently uses unfair commercial practices is a *quantité négligeable*. That is the reason why Article 2 b) UCPD not only holds the trader responsible but also 'anyone acting on behalf or in the name of the trader'. The latter are considered as independent addressees of the UCPD, irrespective of the nature of their legal relationship with the user on whose behalf they act.[232] That is why the user itself is responsible regardless of whether it knows or should have known that externally developed data exploitation strategies are in line with – yet to be concretised – legal requirements.

(178) What if the user engages an auditing company that approves the user's data exploitation strategy or an externally developed one that follows the law? Can the consumer agree with the trader on the processing of their data above and beyond the legally defined threshold? How can such an agreement be integrated as commercial practices before conclusion of a contract and the possibility to ask for consent? Personalisation offers new opportunities for bilateral communication.[233] Just as in contract law, the consumer might have a personal interest in non-compliance, because they expect to benefit from disregard of the legal benchmark. Here we are back to the debate on whether and when the consumer can take a conscious decision. Neither the UCPD nor the UCTD delivers criteria on 'consent'. This is done by the GDPR alone. Consent must be given freely, and must be specific, informed and unambiguous (Articles 4 (11), 7 (4)), and freely revocable (Article 7 (3)). In line with the holistic perspective, the GDPR rules on consent can be taken as a yardstick also in assessment under the UCPD. The major reason is that the UCPD aims at protecting consumer autonomy.[234]

231 (Philip Hacker 2020), p. 12 though in the context of exploitative targeting.

232 In Germany, it is a matter of who is the addressee of an action for injunction under § 8 (2) UWG (Gesetz gegen den Unlauteren Wettbewerb)

233 This aspect is deepened in Area 2 'personalisation of prices and commercial practices'.

234 (Micklitz 2006) Hacker, Manipulating Algorithms, p. 13.

8. What remains for the national courts

(179) The blacklist is meant to provide an exhaustive list of commercial practices which are *per se* prohibited. What does *per se* mean? Does it mean that the CJEU is empowered to make a final decision? Certainly not. In the few judgments which have shaped interpretation of blacklisted practices, the CJEU insisted on the need for the national court to examine whether and to what extent blameworthy practices comply with the legal requirements that the CJEU has formulated. Therefore, 'per se prohibited' does not mean that these practices are prohibited throughout the EU. The competence order of the Treaty enables deviating national court decisions. Conceptually: What is the difference between *per se* prohibited aggressive practices and aggressive practices that take 'account of all its features and circumstances', in the meaning of Article 8? Courts and scholarship draw a distinction between *abstract* malpractices, those blacklisted in the Annex such as health related prohibitions in Member State legal orders, and rules that require courts to consider the *concrete* facts of the case in question.

(180) As there are no blacklisted practices that allow assessment of data exploitation strategies, the CJEU would have to focus on the reach of Articles 8 and 9. *Wind Tre* turned on Italian law that prohibited default settings in the telecommunication sector 'under all circumstances'. Both the AG and the Court insisted that it is for the European legislature alone to decide on possible *per se* prohibitions This reasoning results from full harmonisation of commercial practices in the UCPD.[235] The effect of the two judgments is paradoxical, though. Italy is prevented from introducing *per se* prohibitions. At the same time, the CJEU has no adjudicatory power to decide on the conditions under which a fully harmonized *per se* prohibition applies. Through interpretation of respective EU law the CJEU can only provide guidance to national courts. Even if there is a *per se* prohibition at the European level, the CJEU will still have to delegate the final decision back to the national courts.

(181) Therefore understanding the *structural* asymmetry which is inherent in data exploitation strategies as potentially unfair is just the first building block. Within the scope of Articles 8 and 9, structural asymmetry needs to be complemented by 'additional practices' which point beyond the mere existence of data exploitation strategies These additional practices must be 'undue', not unfair as the German version of *Orange Polska* suggests. If Article 5 UCPD turns into the benchmark, the same issues arise. There must be circumstances which concretise the presumption of unfairness. But what could be the 'additional practices' the CJEU required in *Orange Polska*? A particular design element which renders a data exploitation strategy deliberately problematic, as documented by the Norwegian Consumer

235 The argument is well-known from Austrian-German litigation on per se prohibitions on health related advertising.

Council?[236] Additional practices do not overcome inbuilt structural asymmetry, the incapability of the consumer to understand what is behind the rationale of a data exploitation strategy. The problems do not end here. The additional circumstances must significantly impair the consumer. What, then, is to be regarded as 'significant' in digital commercial practices? Can there really be some stronger impairment than structural asymmetry against which the consumer has no means of defending their rights?

(182) Throughout the two judgments on aggressive practices, the CJEU highlights the residual power of the national courts to investigate whether interpretation of EU law leads to the unlawfulness of a blameworthy practice in the particular case. Therefore clear and specific factual additional practices are needed.[237] Just as in the case law on the UCTD, the CJEU has provided guidance on how these potential concrete circumstances might look like so as to indicate to the referring court at what point the line to an unlawful practice could be crossed. The Court is well advised to do so if it is aiming at a high degree of homogeneity in the final decisions of national courts.

(183) The parallel to standard terms might help to highlight the difference between *structural* aggression and *situational* aggression. The UCTD empowers 'qualified entities' – consumer agencies and consumer organisations – to go to court and test the legality of standard terms *in abstracto*, i.e. without taking into account the individual contract in which standard terms are integrated. The strong insistence of the CJEU on concrete additional circumstances puts the control regime of the UCPD at risk. Just as with standard terms, the CJEU must uphold the distinction between standardised practices and individual practices and develop criteria for both strands of control.

9. 'Normtatsachen (norm facts)', burden of argumentation and burden of proof

(184) In practice, distribution of the burden of argumentation or the burden of proof is all too often much more important than sophisticated legal debate. In the digital economy and digital society, the burden becomes unmanageable, as has been amply demonstrated in sections 1 and 2. These findings are fully confirmed through a parallel discourse in US law. The law on unfair commercial practices has to be rethought in order to remain a useful tool in the fight against digital asymmetry. The key to such a rethink is reversal of the burden of

236 (Norwegian Consumer Council 2018)

237 See also CJEU C-853/19 Order of the Court (Ninth Chamber) of 2 July 2020 IM v Sting Reality s.r.o. Request for a preliminary ruling from the Okresný súd Poprad, ECLI:EU:C:2020:522 at 44 and 59.

argumentation/burden of proof as a necessary consequence of the way in which new technology is used to manipulate the consumer through all sorts of marketing strategies.[238]

(185) Directive 2005/29/EC does not regulate the burden of proof. Recital 21 reads:

> While it is for national law to determine the burden of proof, it is appropriate to enable courts and administrative authorities to require traders to produce evidence as to the accuracy of factual claims they have made.

(186) The UCTD imposes the burden of proof that standard terms are individually negotiated onto the user of standard terms. The GDPR does not contain general rules on how the burden of proof is shared between the processor (the user) and the data subject (the consumer). The benchmark for testing the legality of data processing is bound to the conditions under which personal data are collected be it via the consent of the consumer or through other legitimate forms of data collection (Article 6 GDPR). In case of conflict, the processor (user) must demonstrate that collection and processing of data was lawful. The GDPR does not oblige the processor (user) to demonstrate to the data subject (the consumer), what kind of measures it has taken to comply with the law. This would mean, for the processor (user), disclosing a 'business secret', namely the algorithm which stands behind data exploitation strategies. Here is not the place to discuss the reach and the legitimacy of disclosure duties. What matters is that Articles 35et seq. compensate for such a lacuna. Companies have to produce an impact assessment if there is a high risk to the rights and freedoms of natural persons. The controller must consult the supervisory authorities.[239] These two references in the UCTD and the GDPR could be read so as to indicate the direction where the solution could be found. But is it justifiable to draw a conclusion from the *acquis* on how the burden of proof has to be shared? The most prominent and affirmative example is non-discrimination law, where the Court reversed the burden of proof *de lege lata*. However, reversal only relates to causation between the special characteristics of the potential victim and different treatment. The consumer must still prove different treatment as such,[240] a benchmark that the consumer is unable to hit in default settings.

(187) However, there is a way to overcome the doctrinal difficulties which result from the fact that the UCPD requires consumer agencies and consumer organisations to prove that data exploitation strategies are aggressive in the meaning of Articles 8 and 9, or infringe professional diligence under Article 5. One might understand the data exploitation strategies and the technological infrastructure behind what German lawyers call 'Normtatsachen' – facts which courts need to know in order to interpret general clauses and indeterminate

---

238 (Willis 2020), with regard to personalization strategies H.-W. Micklitz/P. Rott, Personalised Prices and Personalised Marketing, BEUC Study 2020

239 It would be worth studying how companies and supervisory authorities are implementing these obligations.

240 P. Rott, A Consumer Perspective on Algorithms, in L. de Almeida, M. Cantero Gamita, M. Durovic, K. Purnhagen (eds.), The Fransformation of Economic Law, 2019, p. 43.

legal concepts.[241] A classic example would be standard contract terms or boilerplate contracts. Courts are interpreting these terms and contracts as if they were 'law'. They use the same interpretation toolbox. Treating digital asymmetry inherent in data exploitation strategies as 'Normtatsachen' implies that courts are supposed to know and to understand the relevant phenomena. Again, a parallel with standard terms might be useful. Here the CJEU has developed *ex officio* control.[242] Courts must investigate the fairness of standard terms, even if they have not been asked by the parties, in particular by the consumer, to do so.

(188) Transferred to data exploitation strategies, this means that they are to be regarded as a form of regulation that courts have to investigate *ex officio*. Courts suffer from the same universal vulnerability though. Judges are not smarter than the parties before the court. The *ex officio* rule could be extended and adjusted to the particularities of digital asymmetry, though. If properly interpreted, it would allow judges to raise questions as to how technological infrastructure is built, what kind of algorithms are used, and whether the decision is taken by a machine and/or checked by a human being, how exactly the data are technically processed and how they are evaluated, so as to assess the lawfulness of data exploitation strategies with due regard to protection of business secrets. By now courts behave *as if* they understand the technological infrastructure, *as if* it was possible for the user to disclose what the data are used for and for the consumer to understand potential explanations. The judgments dealing with external-structural digital asymmetry are governed by an *as if* ideology.

(189) Turning to the role of the parties, two possible consequences are imaginable: reversal of the *burden of argumentation* or, more ambitiously, reversal of the *burden of proof,* although the two are difficult to distinguish. Reversal of the burden of argumentation/proof implies that the unfairness of data exploitation strategies is presumed and that it would be for the supplier of a digital service to demonstrate that it complies with the law. This could be done through an impact assessment by the controller under the GDPR or through a certificate provided by an auditor. The European Commission has paved the way for the latter option in its latest Communication on the interpretation of the UCPD. However, there is no indication in the CJEU case law that indicates the readiness of the CJEU to limit the freedom of Member States to place the burden of argumentation/proof on the consumer and/or consumer organisations.

---

241 (Schmidt 1985; Sander 1996) Eike Schmidt, *Der Umgang mit Normtatsachen im Zivilprozeß*. In: Christian Broda (Hrsg.): *Festschrift für Rudolf Wassermann zum sechzigsten Geburtstag.* Luchterhand, Neuwied/ Darmstadt 1985, 807–818; Jürgen H. A. Sander: *Normtatsachen im Zivilprozeß*. Duncker & Humblot Verlag, Berlin 1996, Helmut Rüßmann, KritV 1991, 402–415.

242 CJEU from Océano onwards, (Micklitz and Reich 2014)

10. A new yardstick for control

(190) The analysis has revealed serious deficiencies in proper handling of digital vulnerability. The legal system is simply not designed so as to handle external structural universal vulnerability. The position of the consumer is further complicated through the existence of three legislative measures which are co-ordinated neither at the substantive nor at the enforcement level.

- The GDPR, the UCPD and the UCTD should be understood as laying down a common field of fairness at both substantive and enforcement levels. All three legislative measures can be broken down into requirements on standardisation and individualisation of legal relations. This holistic perspective allows for finding commonalities and for a mutual transfer of the rights of consumers, whilst respecting the particularities of each legislative measure.
- Data exploitation strategies *structurally* disadvantage the consumer and are apt to infringe the consumer's rights. The autonomy of the consumer can only be safeguarded if the burden of proof/burden of argumentation is shifted towards the processer/user. The processor/user must show that data exploitation strategies respect legal requirements.
- The processor/user can do so via producing the necessary evidence that the technological infrastructure does not infringe the law or via delegating this screening process to an auditor, who needs to be accredited and whose activities need to be supervised by statutory agencies.

(191) Neither reversing the burden of argumentation/burden of proof nor outsourcing compliance to an auditor solves the problem that external structural disadvantage can only be qualified as unfair if there is evidence that the data exploitation strategy is designed so as to infringe the collective and/or individual rights of consumers. Therefore what is needed are legal requirements that concretise what is meant by aggressive practices and what exactly professional diligence implies in relation to data exploitation strategies.

(192) Two different options present themselves as to how the UCPD could be turned into such an urgently needed instrument: either through blacklisting practices, in line with the *per se* prohibitions enumerated in Annex I, or through elaboration of criteria along the line of a co-design of regulation that duly considers the different role and functions of business, enforcement authorities, and consumer organisations. The Omnibus Directive has not helped to overcome that gap. The EU legislature failed to introduce a comitology procedure which would have allowed a much speedier adaption process. That is why the European Commission is requested to bring together the different stakeholder groups to develop a common set of criteria. However, the new approach type of co-regulation should not be transferred to the digital economy and society without serious re-consideration of the role and function of organisations from civil society. These need to be actively involved in co-

design of the rules, contrary to the new approach where their role is reduced to that of observers.

11. Recommendations

(193) Regulatory concepts:

- Digital vulnerability and digital asymmetry could be anchored in the legislative framework UCDP *de lege lata* i.e. in Articles 5, 8 and 9.
- Reversal of the burden of proof/burden of argumentation for data exploitation strategies could be derived from the UCPD *de lege lata*.
- It would facilitate and accelerate the adaption process of the UCPD to the digital economy and society if both rules were written down in a revised UCPD.

(194) Blacklisted commercial digital practices to be integrated into the Annex under a separate heading:

- Building digital exploitation strategies that claim to serve non-economic interests whereas the overall purpose is commercial.
- Building digital exploitation strategies that establish, maintain, and reinforce situational monopolies
- Building digital situational monopolies that actively discourage users from exercising their right to data portability or switching to other services.
- Use of psychographic profiles to exercise emotional or psychological pressure with the goal of selling products.
- Use of digital exploitation strategies that prevent consumers from invoking consumer law remedies such as annulment of the contract.

(195) New governance on co-design of regulation to concretise legal benchmarks:

- Businesses, consumers, and supervisory agencies need guidelines that concretise a benchmark against which digital exploitation strategies can be measured.
- These rules should be co-designed by businesses, consumer organisations and statutory authorities.
- Processors/traders who comply with co-designed rules are presumed to apply legally acceptable data exploitation strategies.

References

Acquisti, A., L. Brandimarte, and G. Loewenstein. 2015. 'Privacy and Human Behavior in the Age of Information.' *Science* 347 (6221): 509–14. https://doi.org/10.1126/science.aaa1465.

Acquisti, A., and J. Grossklags. 2005. 'Privacy and Rationality in Individual Decision Making.' *IEEE Security and Privacy Magazine* 3 (1): 26–33. https://doi.org/10.1109/MSP.2005.22.

Adjerid, Idris, Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2013. 'Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency.' In *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*, 1. Newcastle, United Kingdom: ACM Press. https://doi.org/10.1145/2501604.2501613.

Advisory Council of Consumer Affairs to the German Federal Ministry of Justice and Consumer Protection. n.d. 'Report of the Advisory Council of Consumer Affairs to the German Federal Ministry of Justice and Consumer Protection: Consumer Law 2.0. Consumers in the Digital World.' https://www.svr-verbraucherfragen.de/en/wp-content/uploads/sites/2/Report-1.pdf.

Albertson Fineman, Martha. 2008. 'The Vulnerable Subject: Anchoring Equality in the Human Condition Essay.' *Yale Journal of Law and Feminism* 20 (1): 1–24.

'An Introduction to Data Mining.' 2014. In *Discovering Knowledge in Data*, by Daniel T. Larose and Chantal D. Larose, 1–15. Hoboken, NJ, USA: John Wiley & Sons, Inc. https://doi.org/10.1002/9781118874059.ch1.

Anderson, J.H. 2014. 'Autonomy and Vulnerability Entwined.' In *Vulnerability: New Essays in Ethics and Feminist Philosophy*, edited by Catriona Mackenzie. Studies in Feminist Philosophy. New York: Oxford University Press.

Ariely, Dan. 2008. *Predictably Irrational: The Hidden Forces That Shape Our Decisions*. 1st ed. New York, NY: Harper Audio.

Audrey R Chapman, and Benjamin Carbonetti. 2011. 'Human Rights Protections for Vulnerable and Disadvantaged Groups: The Contributions of the UN Committee on Economic, Social and Cultural Rights.' *Human Rights Quarterly* 33 (3): 682–732. https://doi.org/10.1353/hrq.2011.0033.

Baier, Annette. 1986. 'Trust and Antitrust.' *Ethics* 96 (2): 231–60. https://doi.org/10.1086/292745.

Baker, Stacey Menzel, James W. Gentry, and Terri L. Rittenburg. 2005. 'Building Understanding of the Domain of Consumer Vulnerability.' *Journal of Macromarketing* 25 (2): 128–39. https://doi.org/10.1177/0276146705280622.

Banas, John A., and Stephen A. Rains. 2010. 'A Meta-Analysis of Research on Inoculation Theory.' *Communication Monographs* 77 (3): 281–311. https://doi.org/10.1080/03637751003758193.

Bartl, Marija. 2010. 'The Affordability of Energy: How Much Protection for the Vulnerable Consumers?' *Journal of Consumer Policy* 33 (3): 225–45. https://doi.org/10.1007/s10603-009-9122-9.

———. 2015. 'Internal Market Rationality, Private Law and the Direction of the Union: Resuscitating the Market as the Object of the Political: Internal Market Rationality.' *European Law Journal* 21 (5): 572–98. https://doi.org/10.1111/eulj.12122.

Baruh, Lemi, Ekin Secinti, and Zeynep Cemalcilar. 2017. 'Online Privacy Concerns and Privacy Management: A Meta-Analytical Review: Privacy Concerns Meta-Analysis.' *Journal of Communication* 67 (1): 26–53. https://doi.org/10.1111/jcom.12276.

Ben-Shahar, Omri. 2009. 'The Myth of the 'Opportunity to Read' in Contract Law.' *European Review of Contract Law* 5 (1): 1–28. https://doi.org/10.1515/ERCL.2009.1.

Berg, Lisbet. 2015. 'Consumer Vulnerability: Are Older People More Vulnerable as Consumers than Others?' *International Journal of Consumer Studies* 39 (4): 284–93. https://doi.org/10.1111/ijcs.12182.

Boerman, Sophie C., Sanne Kruikemeier, and Frederik J. Zuiderveen Borgesius. 2017. 'Online Behavioral Advertising: A Literature Review and Research Agenda.' *Journal of Advertising* 46 (3): 363–76. https://doi.org/10.1080/00913367.2017.1339368.

Bol, Nadine, Tobias Dienlin, Sanne Kruikemeier, Marijn Sax, Sophie C Boerman, Joanna Strycharz, Natali Helberger, and Claes H de Vreese. 2018. 'Understanding the Effects of Personalization as a Privacy Calculus: Analyzing Self-Disclosure Across Health, News, and Commerce Contexts†.' *Journal of Computer-Mediated Communication* 23 (6): 370–88. https://doi.org/10.1093/jcmc/zmy020.

Burkell, Jacqueline and Priscilla M. Regan. 2019. "Voter preferences, voter manipulation, voter analytics: policy options for less surveillance and more autonomy." Internet Policy Review 8(4): 1-24. https://doi.org/10.14763/2019.4.1438

Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein. 2013. 'Misplaced Confidences: Privacy and the Control Paradox.' *Social Psychological and Personality Science* 4 (3): 340–47. https://doi.org/10.1177/1948550612455931.

Calo, Ryan. 2013. 'Digital Market Manipulation.' *University of Washington School of Law Research Paper Nr 2013-27* 82 (4): 995.

———. 2017. 'Privacy, Vulnerability, and Affordance.' *The De Paul Law Review* 66 (2): 591–604.

Cara, Corina. 2019. 'DARK PATTERNS IN THE MEDIA: A SYSTEMATIC REVIEW.' *Network Intelligence Studies* VII (14 (2/2019)): 105–13.

Caronna, F. 2018. 'Tackling Aggressive Commercial Practices: Court of Justice Case Law on the Unfair Commercial Practices Directive 10 Years On.' *European Law Review* 43 (December): 880–903.

Cartwright, Peter. 2015. 'Understanding and Protecting Vulnerable Financial Consumers.' *Journal of Consumer Policy* 38 (2): 119–138. https://doi.org/10.1007/s10603-014-9278-9.

Carver, Charles S., Michael F. Scheier, and Jagdish Kumari Weintraub. 1989. 'Assessing Coping Strategies: A Theoretically Based Approach.' *Journal of Personality and Social Psychology* 56 (2): 267–283. https://doi.org/10.1037/0022-3514.56.2.267.

Chivukula, Shruthi Sai, Chris Watkins, Lucca McKay, and Colin M. Gray. 2019. ''Nothing Comes Before Profit': Asshole Design In the Wild.' In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–6. Glasgow Scotland Uk: ACM. https://doi.org/10.1145/3290607.3312863.

Choi, Hanbyul, Jonghwa Park, and Yoonhyuk Jung. 2018. 'The Role of Privacy Fatigue in Online Privacy Behavior.' *Computers in Human Behavior* 81 (April): 42–51. https://doi.org/10.1016/j.chb.2017.12.001.

Clifford, Damian, and Jef Ausloos. 2017. 'Data Protection and the Role of Fairness.' SSRN Scholarly Paper ID 3013139. Rochester, NY: Social Science Research Network. https://doi.org/10.2139/ssrn.3013139.

Clifford, Damian, Inge Graef, and Peggy Valcke. 2019. 'Pre-Formulated Declarations of Data Subject Consent: Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections.' *German Law Journal* 20 (5): 679–721. https://doi.org/10.1017/glj.2019.56.

Cole, Alyson. 2016. 'All of Us Are Vulnerable, But Some Are More Vulnerable than Others: The Political Ambiguity of Vulnerability Studies, an Ambivalent Critique.' *Critical Horizons* 17 (2): 260–77. https://doi.org/10.1080/14409917.2016.1153896.

Cooper, Frank. 2015. 'Always Already Suspect: Revising Vulnerability Theory.' *North Carolina Law Review* 93 (5): 1339.

Costa-Cabral, Francisco, and Orla Lynskey. 2017. 'Family Ties: The Intersection between Data Protection and Competition in EU Law.' *Common Market Law Review* 54 (1): 11–50.

Couldry, Nick, and Andreas Hepp. 2016. *The Mediated Construction of Reality*. Cambridge, UK ; Malden, MA: Polity Press.

Cox, Kate. 2020. 'Unredacted Suit Shows Google's Own Engineers Confused by Privacy Settings.' Ars Technica. August 25, 2020. https://arstechnica.com/tech-policy/2020/08/unredacted-suit-shows-googles-own-engineers-confused-by-privacy-settings/.

Craig Smith, N., and E. Cooper-Martin. 1997. 'Ethics and Target Marketing: The Role of Product Harm and Consumer Vulnerability.' *Journal of Marketing* 61 (July): 1–20.

Cranor, Lorrie Faith. 2012. 'Can Users Control Online Behavioral Advertising Effectively?' *IEEE Security & Privacy Magazine* 10 (2): 93–96. https://doi.org/10.1109/MSP.2012.32.

Custers, Bart. 2016. 'Click Here to Consent Forever: Expiry Dates for Informed Consent.' *Big Data & Society* 3 (1): 205395171562493. https://doi.org/10.1177/2053951715624935.

Custers, Bart, Francien Dechesne, Wolter Pieters, Bart Schermer, and Simone van der Hof. 2018. 'Consent and Privacy.' In *The Routledge Handbook of the Ethics of Consent*, edited by Andreas Müller and Peter Schaber, 1st ed., 247–58. Routledge. https://doi.org/10.4324/9781351028264-23.

Davies, Gareth. 2013. 'Freedom of Contract and the Horizontal Effect of Free Movement Law'.' In *Involvement of EU Law in Private Law Relationships*, edited by Dorota Leczykiewicz and Stephen Weatherill, 53–70. Studies of the Oxford Institute of European and Comparative Law, v. 16. Oxford, United Kingdom: Hart Pub.

———. 2015a. 'Social Legitimacy and Purposive Power: The End, the Means and the Consent of the People.' In *Europe's Justice Deficit?*, edited by Dimitry Kochenov, G. De Búrca, and Andrew Williams, 259–76. Oxford ; Portland, Oregon: Hart Publishing.

———. 2015b. 'Democracy and Legitimacy in the Shadow of Purposive Competence.' *European Law Journal* 21 (1): 2–22. https://doi.org/10.1111/eulj.12079.

Degeling, Martin, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. 2019. 'We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy.' In *Proceedings 2019 Network and Distributed System Security Symposium*. San Diego, CA: Internet Society. https://doi.org/10.14722/ndss.2019.23378.

Dencik, Lina, Joanna Redden, Arne Hintz, and Harry Warne. 2019. 'The 'Golden View': Data-Driven Governance in the Scoring Society.' *Internet Policy Review* 8 (2). https://policyreview.info/articles/analysis/golden-view-data-driven-governance-scoring-society.

Dijck, José van, Thomas Poell, and Martijn de Waal. 2018. *The Platform Society: Public Values in a Connective World*. Oxford, New York: Oxford University Press.

Duivenvoorde, B.B., and CSECL (FdR). 2015. *The Consumer Benchmarks in the Unfair Commercial Practices Directive*. Springer. https://dare.uva.nl/personal/pure/en/publications/the-consumer-benchmarks-in-the-unfair-commercial-practices-directive(1318aaf2-6c62-435f-9891-88280a4cd394).html.

Duivenvoorde, Bram. 2013. 'The Protection of Vulnerable Consumers under the Unfair Commercial Practices Directive.' *Journal of European Consumer and Market Law* 2 (2): 69–79.

EDPB. 2020. 'Guidelines 8/2020 on the Targeting of Social Media Users.' Guidelines. Brussels: European Data Protection Board (EDPB). https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf.

Everson, M. 1995. 'The Legacy of the Market Citizen.' In *New Legal Dynamics of European Union*, edited by Jo Shaw and Gillian More, 73–90. New York: Clarendon Press.

Everson, Michelle, and Christian Joerges. 2006. 'Consumer Citizenship in Postnational Constellations?' Working Paper. EUI Working Paper Law No. 47. European University Institute. https://cadmus.eui.eu//handle/1814/6547.

Eyal, Nir. 2014. *Hooked: How to Build Habit-Forming Products*. New York, New York: Portfolio/Penguin.

Faden, R. R, and T.L. Beauchamp. 1986. *A History and Theory of Informed Consent*. New York: Oxford University Press. http://www.tandfonline.com/doi/abs/10.1080/01947648609513478.

Frobrukerradet. 2018. 'Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy.' Olso.

Hacker, Philipp. 2018. 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law.' *Common Market Law Review* 55 (4): 1143–1185.

Hardin, Russell. 1996. 'Trustworthiness.' *Ethics* 107 (1): 26–42. https://doi.org/10.1086/233695.

Hardy, G.E., D.A. Shapiro, and C.S. Borrill. 1997. 'Fatigue in the Workforce of National Health Service Trusts: Levels of Symptomatology and Links with Minor Psychiatric Disorder, Demographic, Occupational and Work Role Factors.' *Journal of Psychosomatic Research* 43 (1): 83–92. https://doi.org/10.1016/S0022-3999(97)00019-6.

Helberger, N. 2013. 'Form Matters: Informing Consumers Effectively.' https://dare.uva.nl/search?identifier=1cdb1fd9-046c-446d-9b21-5fd7818c99ef.

Helberger, N., F. Zuiderveen Borgesius, and A. Reyna. 2017. 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law.' *Common Market Law Review* 54. https://dare.uva.nl/search?identifier=1957659a-1069-4c59-a913-20ca5dec0cdc.

Helberger, Natali. 2016. 'Profiling and Targeting Consumers in the Internet of Things - A New Challenge for Consumer Law.' In *Digital Revolution: Challenges for Contract Law in Practice*, 135–61. Baden-Baden: Nomos.

———. 2020. 'The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power.' *Digital Journalism* 8 (6): 842–54. https://doi.org/10.1080/21670811.2020.1773888.

Hill, Ronald Paul, and Eesha Sharma. 2020. 'Consumer Vulnerability.' *Journal of Consumer Psychology* 30 (3): 551–70. https://doi.org/10.1002/jcpy.1161.

Hoboken, J., and S. Gürses. 2018. 'Privacy After the Agile Turn.' In *The Cambridge Handbook of Consumer Privacy*, edited by Evan Selinger, Jules Polonetsky, and Omer Tene. Cambridge, United Kingdom ; New York, NY: Cambridge University Press.

Howells, Geraint G., Hans-W. Micklitz, and Thomas Wilhelmsson. 2006. *European Fair Trading Law: The Unfair Commercial Practices Directive*. Markets and the Law. Aldershot, England ; Burlington, VT: Ashgate Pub. Company.

Howells, Geraint G., Christian Twigg-Flesner, and Thomas Wilhelmsson. 2018. *Rethinking EU Consumer Law*. Markets and the Law. Milton Park, Abingdon, Oxon ; New York, NY: Routledge.

IAB. 2020. 'IAB Europe & IAB Tech Lab Release Updated Transparency & Consent Framework.' *IAB Tech Lab* (blog). 2020. https://iabtechlab.com/press-releases/iab-europe-iab-tech-lab-release-updated-transparency-consent-framework/.

James Q Whitman. 2004. 'The Two Western Cultures of Privacy: Dignity versus Liberty.' *The Yale Law Journal* 113 (6): 1151–1221. https://doi.org/10.2139/ssrn.476041.

Johnston, A. 2016. 'Seeking the EU 'Consumer' in Services of General Economic Interest.' In *The Images of the Consumer in EU Law Legislation, Free Movement and Competition Law.*, 93–138. Oxford: Hart Publishing.

Kahneman, Daniel. 2012. *Thinking, Fast and Slow*. London: Penguin Books.

Kaptein, Maurits, Panos Markopoulos, Boris de Ruyter, and Emile Aarts. 2015a. 'Personalizing Persuasive Technologies: Explicit and Implicit Personalization Using Persuasion Profiles.' *International Journal of Human-Computer Studies* 77 (May): 38–51. https://doi.org/10.1016/j.ijhcs.2015.01.004.

———. 2015b. 'Personalizing Persuasive Technologies: Explicit and Implicit Personalization Using Persuasion Profiles.' *International Journal of Human-Computer Studies* 77 (May): 38–51. https://doi.org/10.1016/j.ijhcs.2015.01.004.

Kelley, Patrick Gage, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. 'A 'Nutrition Label' for Privacy.' In *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*, 1. Mountain View, California: ACM Press. https://doi.org/10.1145/1572532.1572538.

Langenderfer, Jeff, and Terence A. Shimp. 2001. 'Consumer Vulnerability to Scams, Swindles, and Fraud: A New Theory of Visceral Influences on Persuasion.' *Psychology & Marketing* 18 (7): 763–83. https://doi.org/10.1002/mar.1029.

Laufer, Robert S., and Maxine Wolfe. 1977. 'Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory.' *Journal of Social Issues* 33 (3): 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x.

Leczykiewicz, Dorota, and Stephen Weatherill. 2016. *The Images of the Consumer in EU Law Legislation, Free Movement and Competition Law.* London: Bloomsbury Publishing Plc.

Lele, Milind M. 2003. "Monopoly Thinking Can Make Your R&D More Effective. Technology Management: 34-42.

Lutz, Christoph, Christian Pieter Hoffmann, and Giulia Ranzini. 2020. 'Data Capitalism and the User: An Exploration of Privacy Cynicism in Germany.' *New Media & Society* 22 (7): 1168–87. https://doi.org/10.1177/1461444820912544.

Mackenzie, C., W. Rogers, and S. Dodds. 2014. 'Introduction: What Is Vulnerability, and Why Does It Matter for Moral Theory?' In *Vulnerability: New Essays in Ethics and Feminist Philosophy*, 1–29. Studies in Feminist Philosophy. New York: Oxford University Press.

Malgieri, Gianclaudio, and Jędrzej Niklas. 2020. 'Vulnerable Data Subjects.' *Computer Law & Security Review* 37: 105415-. https://doi.org/10.1016/j.clsr.2020.105415.

Mathur, Arunesh, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites.' *Proceedings of the ACM on Human-Computer Interaction* 3 (CSCW): 1–32. https://doi.org/10.1145/3359183.

Matz, Sandra C, Ruth E Appel, and Michal Kosinski. 2020. 'Privacy in the Age of Psychological Targeting.' *Current Opinion in Psychology* 31 (February): 116–21. https://doi.org/10.1016/j.copsyc.2019.08.010.

Matzner, Tobias, Philipp K. Masur, Carsten Ochs, and Thilo von Pape. 2016. 'Do-It-Yourself Data Protection—Empowerment or Burden?' In *Data Protection on the Move*, edited by Serge Gutwirth, Ronald Leenes, and Paul De Hert, 24:277–305. Law, Governance and Technology Series. Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-94-017-7376-8_11.

McGuire, W. 1964. 'Inducing Resistance to Persuasion.' In *Cognitive Theories in Social Psychology: Papers from Advances in Experimental Social Psychology*, edited by Leonard Berkowitz and Norman H. Anderson, 191–229. New York: Academic Press.

Meppelink, Corine S, Julia CM van Weert, Carola J Haven, and Edith G Smit. 2015. 'The Effectiveness of Health Animations in Audiences With Different Health Literacy Levels: An Experimental Study.' *Journal of Medical Internet Research* 17 (1): e11. https://doi.org/10.2196/jmir.3979.

Metzger, Miriam J. 2006. 'Effects of Site, Vendor, and Consumer Characteristics on Web Site Trust and Disclosure.' *Communication Research* 33 (3): 155–79. https://doi.org/10.1177/0093650206287076.

Metzger, Miriam J., and Sharon Docter. 2003. 'Public Opinion and Policy Initiatives for Online Privacy Protection.' *Journal of Broadcasting & Electronic Media* 47 (3): 350–74. https://doi.org/10.1207/s15506878jobem4703_3.

Micklitz, Hans-W. 2006. 'Unfair Practices and Misleading Advertising.' In *European Fair Trading Law: The Unfair Commercial Practices Directive*, 83, 102, 104. Markets and the Law. Aldershot, England ; Burlington, VT: Ashgate Pub. Company.

———. 2007. 'Some Considerations on Cassis de Dijon and the Control of Unfair Contract Terms in Consumer Contracts'.' In *The Future of European Contract Law*, edited by Katharina Boele-Woelki, F. W. Grosheide, and E. H. Hondius, 387–410. Alphen aan den Rijn : Frederick, MD: Wolters Kluwer Law & Business ; Sold and distributed in North, Central, and South America by Aspen Publishers.

———. 2008. 'Some Considerations on Cassis de Dijon and the Control of Unfair Contract Terms in Consumer Contracts'.' In *Standard Contract Terms in Europe: A Basis for and a Challenge to European Contract Law*, edited by Hugh Collins, 19–42. Private Law in European Context Series, v. 15. Alphen Aan Den Rijn : Frederick, Md: Kluwer Law International ; Sold and distributed in North, Central and South America by Aspen Publishers, Inc.

———. 2011. 'German Constitutional Court (Bundesverfassungsgericht BVerfG) 2 BvE 2/08, 30. 6. 2009 – Organstreit Proceedings between Members of the German Parliament and the Federal Government.' *European Review of Contract Law* 7 (4): 528–46. https://doi.org/10.1515/ercl.2011.528.

———. 2014. 'Unfair Terms in Consumer Contracts.' In *European Consumer Law*, by Norbert Reich, Peter Rott, and Klaus Tonner, 2nd edition. Ius Communitatis Series, volume 5. Cambridge: Intersentia.

———. 2018. In *The Politics of Justice in European Private Law*, 329–31. Cambridge Studies in European Law and Policy. Cambridge [UK] ; New York, NY: Cambridge University Press.

Micklitz, Hans-W., and Norbert Reich. 2014. 'The Court and Sleeping Beauty: The Revival of the Unfair Contract Terms Directive (UCTD).' *Common Market Law Review* 51 (3): 771–808.

Micklitz, Hans-W., Anne-Lise Sibony, and Fabrizio Esposito, eds. 2018. *Research Methods in Consumer Law: A Handbook*. Handbooks of Research Methods in Law. Cheltenham, UK; Northampton, MA, USA: Edward Elgar Publishing.

Micklitz, and Monika Namyslowska. 2020a. 'Münchener Kommentar Zum Lauterkeitsrecht, Art. 8 Rdnr. 22.' In .

———. 2020b. 'Münchener Kommentar Zum Lauterkeitsrecht, Art. 8 Rdnr. 26.' In .

Milne, George R., Mary J. Culnan, and Henry Greene. 2006. 'A Longitudinal Assessment of Online Privacy Notice Readability.' *Journal of Public Policy & Marketing* 25 (2): 238–49. https://doi.org/10.1509/jppm.25.2.238.

Nic Shuibhne, Niamh. 2010. 'The Resilience of EU Market Citizenship.' *Common Market Law Review* 47 (6): 1597–1628.

Nickel, P.J. 2015. 'Designing for the Value of Trust. In J. van Der Hoven, P.E. Vermaas & I. Van Der Poel (Eds.), Handbook of Ethics, Values, and Technological Design (Pp. 551-567). Dordrecht: Springer.' In *J. van Der Hoven, P.E. Vermaas & I. Van Der Poel (Eds.), Handbook of Ethics, Values, and Technological Design*, 551–67. Dordrecht: Springer.

Noort, Guda Van, Peter Kerkhof, and Bob M. Fennis. 2008. 'The Persuasiveness of Online Safety Cues: The Impact of Prevention Focus Compatibility of Web Content on Consumers' Risk Perceptions, Attitudes, and Intentions.' *Journal of Interactive Marketing* 22 (4): 58–72. https://doi.org/10.1002/dir.20121.

Nouwens, Midas, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. 'Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence.' In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. Honolulu HI USA: ACM. https://doi.org/10.1145/3313831.3376321.

Park, Yong Jin. 2013. 'Digital Literacy and Privacy Behavior Online.' *Communication Research* 40 (2): 215–36. https://doi.org/10.1177/0093650211418338.

Pasquale, Frank, and Danielle Citron. 2014. 'The Scored Society: Due Process for Automated Predictions.' *Faculty Scholarship* 89 (1): 1–34.

Peroni, L., and A. Timmer. 2013. 'Vulnerable Groups: The Promise of an Emerging Concept in European Human Rights Convention Law.' *International Journal of Constitutional Law* 11 (4): 1056–85. https://doi.org/10.1093/icon/mot042.

Philip Hacker. 2020. 'Manipulation by Algorithms: Exploring the Triangle of Unfair Commercial Practice, Data Protection, and Data Privacy.' Working Paper.

Pollach, Irene. 2005. 'A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent.' *Journal of Business Ethics* 62 (3): 221–35. https://doi.org/10.1007/s10551-005-7898-3.

Poort, Joost, and Frederik J. Zuiderveen Borgesius. 2019. 'Does Everyone Have a Price? Understanding People's Attitude towards Online and Offline Price Discrimination.' *Internet Policy Review* 8 (1). https://doi.org/10.14763/2019.1.1383.

Ray Fisman, and Michael Luca. 2016. 'Fixing Discrimination in Online Marketplaces.' *Harvard Business Review*, 1-.

Reich, N. 2016. 'Vulnerable Consumers in EU Law.' In *The Images of the Consumer in EU Law Legislation, Free Movement and Competition Law.*, 139–58. Oxford: Hart Publishing.

Rössler, Beate, and R. D. V. Glasgow. 2005. *The Value of Privacy*. English ed. Cambridge, UK ; Malden, MA: Polity Press.

Rott, Peter. 2017. 'Data Protection Law as Consumer Law – How Consumer Organisations Can Contribute to the Enforcement of Data Protection Law.' *Journal of European Consumer and Market Law* 6 (3): 113–119.

———, ed. 2019. *Certification - Trust, Accountability, Liability*. 1st ed. 2019. Studies in European Economic Law and Regulation 16. Cham: Springer International Publishing : Imprint: Springer. https://doi.org/10.1007/978-3-030-02499-4.

Ryan, Johnny. 2018. 'French Regulator Shows Deep Flaws in IAB's Consent Framework and RTB.' Brave Browser. November 20, 2018. https://brave.com/cnil-consent-rtb/.

Sander, Jürgen H. A. 1996. *Normtatsachen im Zivilprozeß*. Berlin: Duncker & Humblot Verlag.

Scammell, Margaret. 2000. 'The Internet and Civic Engagement: The Age of the Citizen-Consumer.' *Political Communication* 17 (4): 351–55. https://doi.org/10.1080/10584600050178951.

Schmidt, Eike. 1985. 'Der Umgang mit Normtatsachen im Zivilprozeß.' *Christian Broda (Hrsg.): Festschrift für Rudolf Wassermann zum sechzigsten Geburtstag*, 807–18.

Smit, Edith G., Guda Van Noort, and Hilde A.M. Voorveld. 2014. 'Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns and Online Coping Behaviour in Europe.' *Computers in Human Behavior* 32 (March): 15–22. https://doi.org/10.1016/j.chb.2013.11.008.

Solon Barocas, and Andrew D Selbst. 2016. 'Big Data's Disparate Impact.' *California Law Review* 104 (3): 671–732.

Spindler, Gerald, and Andreas Seidel. 2018. 'Die Zivilrechtlichen Konsequenzen von Big Data Für Wissenszurechnung Und Aufklärungspflichten.' *Neue Juristische Wochenschrift*, no. 30: 2153–57.

Staahb, Philip. 2019. *Digitaler Kapitalismus - Markt Und Herrschaft in Der Ökonomie Der Unknappheit*. 1st ed. Frankfurt am Main: Suhrkamp.

Steinberg, Laurence, and Amanda Sheffield Morris. 2001. 'Adolescent Development.' *Annual Review of Psychology* 52 (1): 83–110. https://doi.org/10.1146/annurev.psych.52.1.83.

Strycharz, Joanna, Jef Ausloos, and Natali Helberger. 2020. 'Data Protection or Data Frustration? Individual Perceptions and Attitudes Towards the GDPR.' *European Data Protection Law Review* 6 (3): 407–21. https://doi.org/10.21552/edpl/2020/3/10.

Strycharz, Joanna, Guda Van Noort, Edith Smit, and Natali Helberger. 2019. 'Protective Behavior against Personalized Ads: Motivation to Turn Personalization Off.' *Cyberpsychology:*

Journal of Psychosocial Research on Cyberspace 13 (2). https://doi.org/10.5817/CP2019-2-1.

Susser, Daniel, Beate Roessler, and Helen Nissenbaum. 2019. 'Technology, Autonomy, and Manipulation.' *Internet Policy Review* 8 (2). https://doi.org/10.14763/2019.2.1410.

Thaler, Richard H. 2015. *Misbehaving: The Making of Behavioral Economics*. First edition. New York: W.W. Norton & Company.

Thaler, Richard H., and Cass R. Sunstein. 2008. *Nudge: Improving Decisions about Health, Wealth, and Happiness*. New Haven: Yale University Press.

Tsebelis, George. 1990. *Nested Games: Rational Choice in Comparative Politics*. Berkeley: University of California Press. https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=42262.

Tyler, Tom R., and Fay L. Cook. 1984. 'The Mass Media and Judgments of Risk: Distinguishing Impact on Personal and Societal Level Judgments.' *Journal of Personality and Social Psychology* 47 (4): 693–708. https://doi.org/10.1037/0022-3514.47.4.693.

Unberath, Hannes, and Angus Johnston. 2007. 'The Double-Headed Approach of the ECJ Concerning Consumer Protection.' *Common Market Law Review* 44 (5): 1237–1284.

Ur, Blase, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. 'Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising.' In *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*, 1. Washington, D.C.: ACM Press. https://doi.org/10.1145/2335356.2335362.

Utz, Christine, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. '(Un)Informed Consent: Studying GDPR Consent Notices in the Field.' In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 973–90. London United Kingdom: ACM. https://doi.org/10.1145/3319535.3354212.

Van Dijck, Jose. 2014. 'Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology.' *Surveillance & Society* 12 (2): 197–208. https://doi.org/10.24908/ss.v12i2.4776.

Waldman, Ari Ezra. 2020. 'Cognitive Biases, Dark Patterns, and the 'Privacy Paradox.'' *Current Opinion in Psychology* 31 (February): 105–9. https://doi.org/10.1016/j.copsyc.2019.08.025.

Wang, Yang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. 2011. ''I Regretted the Minute I Pressed Share': A Qualitative Study of Regrets on Facebook.' In *Proceedings of the Seventh Symposium on Usable Privacy and Security - SOUPS '11*, 1. Pittsburgh, Pennsylvania: ACM Press. https://doi.org/10.1145/2078827.2078841.

Weatherill, St. 2004. 'Competence Creep and Competence Control.' *Yearbook of European Law* 23 (1): 1–55. https://doi.org/10.1093/yel/23.1.1.

Westin, Alan. 1968. 'Privacy And Freedom.' *Washington and Lee Law Review* 25 (1): 166–70.

'What Is Data Protection Policy? - Definition from Techopedia.' 2017. Techopedia.Com. January 23, 2017. http://www.techopedia.com/definition/30183/data-protection-policy.

Wiesemann, C. 2017. 'On the Interrelationship of Vulnerability and Trust.' In *Vulnerability, Autonomy, and Applied Ethics*, edited by Christine Straehle, 1 [edition], 157–70. Routledge Research in Applied Ethics 1. London: Routledge.

Wilhelmsson, Thomas. 2006. 'Harmonizing Unfair Commercial Practices Law: The Cultural and Social Dimensions.' *Osgoode Hall Law Journal (1960)* 44 (3): 461-.

Zuiderveen Borgesius, Frederik. 2014. 'Behavioural Sciences and the Regulation of Privacy on the Internet.' SSRN Scholarly Paper ID 2513771. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2513771.

Zuiderveen Borgesius, Frederik, and Joost Poort. 2017. 'Online Price Discrimination and EU Data Privacy Law.' *Journal of Consumer Policy* 40 (3): 347–66. https://doi.org/10.1007/s10603-017-9354-z.

Part II

Personalised Pricing and Personalised Commercial Practices

Orla Lynskey[1], Hans-W. Micklitz[2] and Peter Rott[3]

---

1 Associate Professor of Law at the LSE and Visiting Professor at the College of Europe, Bruges specialising in Digital Rights and Technology Regulation, in particular EU Data Protection Law.

2 Professor for Economic Law, Robert Schuman Centre for Advanced Studies at the European University Institute and Finland Distinguished Professor, University of Helsinki, with a broad track record in European Private and Economic Law, National and European Consumer Law, Legal Theory.

3 Interim Chair of Civil Law, Commercial Law and Information Law at Carl von Ossietzky University of Oldenburg, Germany.

Part II: Table of Contents

Argument – Area 1 and Area 2[1]

(1) Analysis of personalisation of prices and marketing should be read in conjunction with the key findings in Area 1. Digital vulnerability is universal and structural and justifies reversal of the burden of proof/burden of argumentation. Personalisation through pricing and marketing is nothing more than a variation of the consumer's universal and structural vulnerability. We will show that personalisation increases the structural imbalance, as it is based on data exploitation strategies. Contrary to what the term insinuates, 'personalisation' does not lead to an individualisation that enables the consumer to better defend their rights. Quite the contrary. That is why reliance on informational tools is not only insufficient, but dysfunctional. The following analysis emphasises the structural dimension of personalisation.

(2) The analysis is broken down into three parts – firstly, development of a framework for analysis which combines research on personalisation in marketing and behavioural science with conceptualization of a coherent legal architecture, secondly and thirdly analysis of the current legal framework on personalised pricing followed by personalised commercial practices. Focus on the GDPR, the UCPD, the UCTD and non-discrimination law is meant to set a counterweight against proliferating debates on the 'ifs' and 'hows' of using antitrust law to solve the consumer concern by way of competition.

I. Digital vulnerability, digital asymmetry and personalisation

(3) Personalisation requires enlarging the legal framework beyond the GDPR, the UCPD, and the UCTD towards non-discrimination law. This broadening implies a rethink of the basic distinction between standardisation and individualisation in the control architecture that serves as a starter for development of a common control level for assessing personalised commercial practices. Personalisation does not seem to fit the distinction. That explains the need to clarify the difference between the person/personalisation and the individual/individualisation. We will demonstrate that personalisation is best understood as a pre-designed form of quasi-individualised standardisation, already enshrined in the UCTD and the UCPD.

[1] This paper is a joint contribution which the authors discussed at various stages. Hans-W. Micklitz has written the overall legal framework and the part on personalised commercial practices, except data protection, Peter Rott the part on personalised pricing, and Orla Lynskey the part on data protection law in personalised commercial practices.

1. *Personalisation, digital asymmetry and the EU legal framework*

(4) In area 1, the default settings to be analysed are data exploitation strategies,[2] in area 2 the data exploitation strategies are shaped so as to retrieve data that allow for personalising pricing and personalising marketing. The ground level and the surface level intermingle. The consumer is in the same structural position, being submitted to a predesigned digital architecture and to the power of superior knowledge that they cannot compensate. Personalisation adds a new layer to the technological infrastructure, though. Data exploitation strategies normally address the 'consumer' as a societal entity. The consumer – whoever they may be, male, female, young, old and wherever they live, needs to subscribe to the data exploitation strategy if they want to have access to the internet.

(5) Personalisation goes beyond. Consumers can be broken down into various target groups, up to a point where the consumer is no longer a person but an individual. What remains is the universality of consumer vulnerability. In the digital economy and digital society, each of us – 'consumers we are all'[3] – is the addressee of a rapidly ongoing personalisation. It seems that personalisation is not only the future of all marketing activities but also of the law.[4] This would mean that personalised tailoring of data exploitation strategies, of commercial practices, and of standard contract terms is equally reflected in personalised legal standards. For some this might look like *horror juris*, for others it looks like a future where each consumer gets the law they need.

(6) The relevant legal rules deal neither with personalisation nor with digital vulnerability. Digital vulnerability and personalisation have to be squeezed into data protection (GDPR), unfair commercial practices (UCPD), and unfair contract terms (UCTD) legislation. Personalisation puts the focus on non-discrimination law and fundamental rights. The latter two areas are catapulting consumer law into different spheres, into algorithmic discrimination[5] and into

---

2 With regard to the use and definition of data exploitation strategies see N. Helberger, H. Micklitz, M. Sax and J. Strycharz, *EU Consumer Protection 2.0: Surveillance, consent and the vulnerable consumer. Regaining citizen agency in the information economy, A study for BEUC*, 2020.

3 President Kennedy, 1962, https://en.wikipedia.org/wiki/Consumer_Bill_of_Rights.

4 A. Porat and L.J. Strahilevitz, Personalizing Default Rules and Disclosure with Big Data, 112 *Michigan Law Review* (2014), 1417, available at: http://repository.law.umich.edu/mlr/vol112/iss8/2; P. Hacker, Personalizing EU Private Law: From Disclosures to Nudges and Mandates, *European Review of Private Law* 2017, 651 ff.; A. Porat and O. Ben-Shahar, Personalised Mandatory Rules in Contract Law, 68 *University of Chicago Law Review* (2019), 255 ff:; G. Wagner and H. Eidenmüller, Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalised Transactions, 68 *University of Chicago Law Review* (2019), 581 ff.; N. Elkin-Koren and M.S. Gal, Personalised Law, The Chilling Effect of Governance-by-Data on Data Markets, 68 *University of Chicago Law Review* (2019), 403 ff.; P.M. Bender, Limits of Personalisation of Default Rules – Towards a Normative Theory, *European Review of Contract law* 2020, 366.

5 P. Hacker, Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law, 55 *Common Market Law Review* (2018), 1143 ff.

the constitutionalisation of private law relations through fundamental and human rights.[6] Non-discrimination law is much closer to labour law than to consumer law. Current EU non-discrimination law is composed of five directives: Directive 2000/43/EC on racial equality, Directive 2002/78 framework on employment and occupation, Directive 2004/113/EC on gender equality in provision of goods and services, Directive 2004/38/EC on EU citizens and family members and Directive 2006/54/EC on equal opportunities. Due to strong resistance by the Member States, the European Commission had to withdraw its proposal to extend general non-discrimination law beyond the workplace into economic transactions more generally.[7]

(7) The Draft Common Frame of Reference (DCFR) included non-discrimination law in what should have become, at least in the minds of the drafters, the 'new European Civil Code'. The remainder of the DCFR, the Proposal for a Common European Sales Law, did not cover non-discrimination law. After its withdrawal, the EU finally succeeded in finding support for a revision of the 'New Deal for Consumers'. Neither Directive (EU) 2019/771 nor the Omnibus Directive (EU) 2019/2161 refers to discriminatory practices, though that could affect the consumer. Setting aside constitutionalisation via fundamental and human rights, all that remains is therefore Directive 2004/113/EC which touches upon discriminatory practices of goods and services which are 'available to the public' (Article 3 (1)).

(8) Stock-taking suggests that the five directives are tailored to protect employees against discriminatory practices by employers. However, and in line with the holistic perspective here defended, we start from the assumption that what is unlawful in employment contracts might *prima facie* not be upheld in the GDPR, the UCPD or the UCTD – provided the context so allows. All three legislative means provide for a fairness test that is wide enough to integrate, in principle, discriminatory practices such as those sanctioned under the four Directives. The regulatory prohibitions – provided there is discriminatory practice related to gender, age, race, ethnic origins, or handicap – have to be tested under the good faith clause in Article 3 UCTD, under the professional diligence test in Article 5 UCPD, and under Article 5(1)(a) GDPR, which requires fair and transparent data processing.[8] So theoretically and conceptually it does not and cannot matter where to start from. A much more difficult question is how to interlink the different legal fields. Here the CJEU has provided useful guidance.

---

6 There is an abundant literature, A. Colombi Ciacchi, G. Brüggemeier and G. Comandé (eds), *Fundamental Rights and Private Law in the European Union,* Vol. I and II (Cambridge University Press, 2010); H.-W. Micklitz (ed.), *Constitutionalization of European Private Law* (Oxford University Press, 2014), on non-discrimination law.

7 For an overview from a private law perspective, see H.-W. Micklitz, *Politics of Justice in European Private Law* (Cambridge University Press, 2018), 199 ff.

8 D. Clifford and J. Ausloos, Data Protection and the Role of Fairness, 2017, SSRN Scholarly Paper ID 3013139, https://doi.org/10.2139/ssrn.3013139.

2. *Control architecture - standardisation and individualisation*

(9) Taking digital asymmetry as the starting point, we propose a holistic perspective so as to distil from the various laws a common element of fairness which is understood to be relevant under whatever legal regime. In evaluating data exploitation strategy, we have drawn a distinction between judicial review of standardized versus individualized practices, which we claim to exist in the GDPR, the UCPD and the UCTD. The standardized and the individualized stand side-by-side, within the scope of the UCTD paradigmatically tied together through the case law of the CJEU. The Court leaves it to the consumer to decide *ex post factum* whether they are ready to accept an unlawful standard term because they believe that, overall, they are better off, whatever their reasons might be.[9] Personalisation of prices and marketing – this is the working hypothesis – can and should be analysed along the same distinction. We will first highlight the extended control architecture including non-discrimination law and fundamental rights, before investigating how personalisation fits into the carefully crafted regulatory design.

(10) The extended control architecture would lead to the following setting:

	UCTD Contract terms	UCPD Commercial practices	GDPR Data protection	NDL (non-discrimination law)	FR (fundamental + human rights
Standardized Abstract general	Standardized terms Collective redress	Standardized commercial practices Public/private collective redress	Standardized data privacy policies Public enforcement via the GDPR+ Public/private collective enforcement via the UCPD	Standardised discriminatory pre- + contractual policies Public/private collective redress	Standardized human rights indicator + EU Agency for Fundamental Rights
Individualised Concrete individual	Individually negotiated terms + Individual enforcement	Individualized commercial practices + Individual enforcement	Individual rights to information and explanation + a prohibition on automated decision-making Individual enforcement	Individual rights + judicial protection	Individual rights + judicial protection

9 C. Leone, The missing stone in the Cathedral: Of unfair terms in employment contracts and co-existing rationalities in European contract law (ph.d., Amsterdam, 2020).

(11) The table above complements the one developed and explained in Area 1. All that is needed is to explain why the distinction between standardized and individualized also operates in the field of non-discrimination law and fundamental rights both in substantive law and with regard to redress and why they are linked together in a similar way.

a) Substance

(12) The four directives aim at eliminating discriminatory practices either in employment contracts or in contracts 'addressed to the public'. These practices include denial of a contract. The five Directives do not distinguish between standardised and individualised discriminatory practices. Directive 2004/113/EC addresses individual practices/terms, which may equally be the product of standardisation, whereas Directives 2000/43/EC, 2000/78/EC and 2006/54/EC deal with collective agreements. From a consumer law perspective, Directive 2004/113/EC deserves the utmost attention. How far does 'offered to the public' reach? Typically, public offers precede the contract. Legal doctrine has discussed the offer *ad incertas personas* ever since. However, in reality this is the exception to the rule. A typical example is the 'public' viewing of houses or apartments for rent, where consumers compete with each other in the selection process. So far, no CJEU case law is available that would allow a first concretization.

(13) However, in the widely and controversially discussed *Feryn*[10] judgment, the CJEU had to deal with an advertisement by a Belgian seller of door fitters, who offered a job, but not to 'immigrants' as clients were supposed to fear that their work might endanger the security of their property. The CJEU had no problem in putting the advertising under the scope of Directive 2000/43/EC. *Feryn* could be generalized. All five directives would then cover the pre-contractual stage, which in fact is the phase where it is decided whether the worker/consumer might have a chance to conclude a contract. Therefore the five directives determine what is to be understood as unfair in the meaning of Article 5 UCPD. Any open discrimination because of gender, race, ethnic origin, religion, age and handicap in advertisements is *prima facie* not compatible with EU law.

b) Remedies

(14) The five directives are much less clear on remedies. Despite the proximity to market behaviour as enshrined in Directives 93/13/EEC and 2005/29/EC, the five directives do oblige Member States to introduce collective remedies such as injunctions to eliminate discriminatory practices. The five Directives leave it for the Member States to decide whether and who should exercise such a collective right. It remained for the CJEU in *Feryn* to 'invent' an action for injunction. The CJEU held that the concept of discrimination in

[10] ECJ, 10/7/2008, Case C-54/07 Centrum voor gelijkheid van kansen en voor racismebestrijding v Firma Feryn NV, ECLI:EU:C:2008:397.

Directive 2004/113/EC does not depend 'on the identification of a complainant who claims to have been the victim'.[11] This statement can be extended to the other three non-discrimination Directives where the overall purpose is to eliminate discriminatory practices that bar access to the employment market and to publicly offered contracts that precede conclusion of a contract. Extending the *Feryn* reasoning is even more important as the newly adopted Directive (EU) 2020/1828 on representative actions[12] does not grant standing to consumer agencies and consumer organisations with regard to non-discrimination Directives. However, as discriminatory practices in b2c relations are supposed to be unfair within the scope of the UCPD and the UCTD, consumer agencies and consumer organisations are entitled to eliminate discriminatory practices through an action for injunction.

c) Linking collective and individual judicial review

(15) Unlike the UCTD, the five Non-Discrimination Directives do not link standardised and individual discriminatory practices.[13] However, they contain basic elements that allow for using the established case law of the CJEU on the UCTD as a benchmark. Articles 14 b) Directive 2000/43/EC, Article 16 b) Directive 2000/78/EC,[14] Article 13 b) Directive 2004/113/EC and Article 23(2) Directive 2006/54/EU[15] oblige Member States to take measures to ensure that '*contractual provisions are or may be declared null and void*'. The Directives remain silent on what '*may*' means, in particular whether adjustment of an existing contract to the requirements of non-discrimination law through a court in individual litigation could be a solution. The situation of the socially discriminated – those suffering

---

11 ibid., para. 25.

12 OJ 2020 L 409/1.

13 AG Trstenjak, 29/11/2011, Case C-453/10 Jana Pereničová and Vladislav Perenič v SOS financ spol. s r. o., ECLI:EU:C:2011:788, paras 89-90; CJEU, 15/3/2012, Case C-453/10 Jana Pereničová and Vladislav Perenič v SOS financ spol. s r. o., ECLI:EU:C:2012:144, paras 43-44; Case C-109/17; CJEU, 19/9/2018 Bankia SA v Juan Carlos Mari Merino and Others, ECLI:EU:C:2018:735, para. 49, B. Keirsbilck, Interaction between Consumer Protection Rules on Unfair Contract Terms and Unfair Commercial Practices: Perenicova and Perenic, Common Market Law Review 50 (2013), 247 ff.; H.-W. Micklitz and N. Reich, AGB-Recht und UWG – (endlich) ein Ende des Kästchendenkens nach EuGH Pereničová und Invitel?, *Europäisches Wirtschafts- und Steuerrecht* 2012, 257 ff.

14 Which are identical: According to Art. 14(b) Directive 2000/43/EC, 'Member States shall take measures to ensure that 'any provisions contrary to the principle of equal treatment which are included in individual or collective contracts or agreements, internal rules of undertakings, rules governing profit-making or non-profit-making associations, and rules governing the independent professions and workers' and employers' organisations, are or may be declared, null and void or are amended'. Regarding Art. 16(b) Directive 2000/78/EC, Member States shall ensure that 'any provisions contrary to the principle of equal treatment which are included in contracts or collective agreements, internal rules of undertakings or rules governing the independent occupations and professions and workers' and employers' organisations are, or may be, declared null and void or are amended'.

15 Slightly different wording: According to Art. 13(b) Directive 2004/113/EC, Member States shall ensure that 'any contractual provisions, internal rules of undertakings, and rules governing profit-making or non-profit-making associations contrary to the principle of equal treatment are, or may be, declared null and void or are amended'. Regarding Art. 23(b) Directive 2006/54/EC, Member States shall ensure that 'provisions contrary to the principle of equal treatment in individual or collective contracts or agreements, internal rules of undertakings or rules governing the independent occupations and professions and workers' and employers' organisations or any other arrangements shall be, or may be, declared null and void or are amended'.

from discrimination – is similar to the consumer who has to decide whether they insist on elimination of a contract term which has been declared unlawful in collective proceedings, or whether they accept the unfair term. It seems fair to assume that the CJEU, if asked, would apply a similar reasoning as under the UCTD. Whilst this might be a promising avenue for judicial control of contract terms in existing contracts, the same reasoning cannot easily be transferred to the pre-contractual stage. The internet paves the way for communication between consumer and supplier even before the contract, for instance through chat boxes.[16] Chat boxes are the preferred target of personalised marketing strategies as we will show. The seemingly clear line between marketing and contract is vanishing. If, however, chat boxes are turned into chat bots, personalised communication is substituted through technological standardisation.

d) Fundamental and human rights

(16) What remains to be discussed is the role of fundamental and human rights in the design of control architecture. Extension of non-discrimination law, which is lacking beyond the workplace, directs attention – or even hope depending on one's position – to fundamental and human rights and to their potential direct effect in private law relations, not only in contract law but also in law on commercial practices. For more than 20 years it looked as if it was a long way down the road from bringing discriminatory contractual practices under the scope of Article 21 Charter of Fundamental Rights to a potential direct effect in contractual relations.[17] However, in *Egenberger* and in *Bauer* the CJEU held that Article 21 was sufficient in itself to confer rights on individuals.[18] The remaining barriers are even higher in terms of the impact of fundamental and human rights on commercial practices. However, personalised advertising transforms one-way advertising and marketing into an open bilateral communication between the supplier of commercial practices and the targeted consumer, via chat boxes, via on-site personalisation and via customization.[19] Collective marketing strategies turn into personalised activities targeted at individual customers.

(17) The Charter does not provide for collective rights to enforce fundamental rights. However, the Fundamental Rights Agency could, if legally empowered and properly equipped,

---

16 T. Gausling, Künstliche Intelligenz im digitalen Marketing, Datenschutzrechtliche Bewertung KI-gestützter Kommunkations-Tools and Profiling-Maßnahmen, *Zeitschrift für Datenschutz* 2019, 335, 336.

17 N. Reich, *General Principles of EU Civil Law* (Intersentia, 2014), chapter 2.

18 CJEU, 17/4/2018, Case C-414/16 *Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung eV*, ECLI:EU:C:2018:257, para. 76; confirmed by CJEU, 6/11/2018, joined Cases C-569/16 and C-570/16 *Stadt Wuppertal* v. *Maria Elisabeth Bauer* and *Volker Wilmeroth v Martina Broßonn*, ECLI:EU:C:2018:871, para. 85; P. Rott, Powerful Private Players in the Digital Economy: Between Private Law Freedom and the Constitutional Principle of Equality, *Baltic Yearbook of International Law* 18 (2019), 32 ff, forthcoming; D. Leczykiewicz, The Judgment in *Bauer* and the Effect of the EU Charter of Fundamental Rights in Horizontal Situations, *European Review of Contract Law* 2020, 323 ff.

19 See below where the different techniques of personalisation are explained.

eliminate discriminatory practices. The legal framework under which the Agency operates is miles away from Europeanised legal standards on 'qualified entities' that enforce the UCTD and the UCPD. The Agency has no power to take action, but its assessment might very well unfold practical importance and could be integrated into a fairness test under the UCTD, UCPD and the GDPR.[20]

3. Personalisation between standardisation and individualisation

(18) The key question is whether and to what extent the control architecture which is built on the distinction between standardisation and individualisation collapses with personalization or whether the distinction is based on false premises as the key question should be whether the consumer has had a meaningful chance to impact personalization.[21] The distinction could indeed lose importance if personalisation had to be equated with individualisation. The whole control architecture would have to be adjusted so as to enforce individualized (= personalized) practices not only through individual rights but also through collective rights. Collective entities with legal standing would need powers to act 'on behalf' of the individual. But where should legitimacy be derived from? No interest would reach beyond the concrete problem of the individual as each individual would receive their own data privacy policies, their own commercial practices and their own standard terms.

a) Pre-formulated individual terms/practices

(19) Interestingly enough, both the UCTD and the UCPD point exactly in this direction. Article 3(1) UCTD covers pre-formulated individual terms which address a single consumer.[22] Until now, this category has not been given shape by the CJEU. As far at the UCPD is concerned, the CJEU had no difficulty in submitting commercial practices targeting a single consumer under the scope of application.[23] Directive 2004/113/EC requires that contracts are 'offered to the public'. The formula 'offered to the public' highlights a deeper problem, much discussed in the field of standard terms. Standard terms, if provided by a single company, are not public.

---

20 On the shift from courts to administrative enforcement, see B. de Witte, New Institutions for Promoting Equality in Europe: Legal Transfers, National Bricolage and European Governance, 60 American Journal of Comparative Law (2012), 49 ff.; on the ambiguous consequences of human rights indicators, see A. Beckers, From Corporate Personality to Corporate Governance, The Transformation of International Human Rights Protection in Corporate Governance Structures, in N. Buhta and R. Vallejo (eds), Human Rights and Global Governance, Oxford University Press, Oxford 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3573755.

21 In this direction P. Palka, The World of Fifty (interoperable) Facebooks, *Seton Hall Law Review* 51 (2021), forthcoming.

22 H.-W. Micklitz, Unfair Terms in Consumer Contracts, in N. Reich, H.-W. Micklitz, P. Rott and K. Tonner, *European Consumer Law*, 2nd ed. (Intersentia, 2014), para. 3.8.

23 ECJ, 16/4/2015, Case C-388/13 Nemzeti Fogyasztóvédelmi Hatóság v UPC Magyarország kft, ECLI:EU:C:2015:481.

(20) In France, the consumer authorities are entitled to require disclosure of standard terms, enforced through the courts if needed.[24] In Germany, no such right exists.[25] That is why consumer organisations usually provide evidence through three examples where consumers have been confronted with the same standard terms. But how could the targeted individual consumer or consumer agencies and consumer organisations know whether a particular commercial practice is individualized (=personalized) or still standardized? Directive 2004/113/EC makes public-ness an explicit condition for its applicability. Individualised-personalised discriminatory practices might easily fail this benchmark.

b) The person and the individual

(21) Two ways are available to overcome these difficulties and to keep the control architecture in place as long as we operate within the given regulatory framework:

- firstly, personalisation may be regarded as a standardized practice, even if personalisation can be equated with individualisation;
- secondly, personalisation may be distinguished from individualisation and therefore not call into question the distinction between standardisation and individualisation.

(22) The current debate on personalisation in law[26] and in marketing[27] is mixing up personalisation and individualisation in a bewildering way, up to a point where the two are used interchangeably (discussed in more detail below under 'techniques of personalised commercial practices'). This is not only incorrect but also irritating, as it leads to conceptual confusion. The law distinguishes between the person and the individual. The person is a legal construct. Since adoption of the Code Civil in 1804, the starting point of Western democratic private law orders has been the normative assumption that all persons are born equal and equipped with the same rights. The French language is much clearer than English or German. French law distinguishes between '*le sujet de droit*' (the legal subject) and '*l'individuel*' (the individual). The normative claim enshrined in the legal construct of the 'person' is neither meant to reflect the reality nor to do justice to reality. The gap between the normative claim and socio-economic reality led to the introduction of status-related rights, first for workers, later for consumers, today for the societally discriminated. However, status-related rights carry a heavy normative baggage, too. There is no such thing as the 'worker' or 'the consumer'. Behavioural research breaks down 'the consumer' into ever more fine-grained

---

24 J. Calais-Auloy, Droit de la Consommation, 10th ed. (Dalloz, 2020), 178 f.

25 See BGH, 23/2/2010, XI ZR 186/09, *Neue Juristische Wochenschrift* 2010, 10.

26 To the best of our knowledge, there is no article discussing phenomena of personalisation that clarifies the meaning of personalisation and individualisation.

27 See J. Strycharz, G.v. Noort, N. Helberger and E. Smit, Contrasting perspectives – practitioner's viewpoint on personalised marketing communication, *European Journal of Marketing* 2019, 635, 641: 'Looking at the literature, defining personalisation is not easy; past studies provides us with a number of definitions that are often dramatically different from each other.'

categories, which are only insufficiently reflected in the threefold distinction between the average, the confident, and the vulnerable.[28] This research can be connected to personalization of legal rules.[29]

(23) Clarification is needed on who the individual is and what exactly personalisation produces and how it can or cannot be brought into line with the control architecture:

- Who is the individual? Is the individual a 'real person'?
- What does personalisation do, does it digitalise the 'person' or the 'individual' or both?
- Is digitalization to be understood as standardisation or as individualisation?
- If the person is a normative construct, is personalisation necessarily a normative concept to be kept distinct from the individual?

(24) Individual characteristics make each person unique. That is why the individual, the *personality* of each individual, has to be kept distinct from the person as a normative figure. What is loosely termed personalisation is a composite of four different elements. *First* and foremost are objective data on the birthday, ancestry, age, sex, and place of residence of each and every person. These are individual characteristics. *Secondly*, there are data about *individual* preferences, data that each of us leaves on the internet and that companies are so eager to collect. Each internet user thereby creates their own alter ego, for example a 'person' called HM (Hans Micklitz), composed of HM's *preferences* but which is not HM.[30] Crudely speaking, these data, if they cannot be traced back to an identifiable individual person, provide information about the behaviour of HM-type persons but not about HM's individual personality. That is why it is possible, and even sometimes advocated, to operate through different individual behavioural preferences (alter ego HM 1 and alter ego HM 2) so as to check whether there are differences in personalised prices. Can the alter ego be called an individual at all and if it is called a person what does this imply? *Thirdly*, there are data on our social ties – replicating the famous saying 'tell me who your friends are and I tell you who you are'. So who are HM's friends and colleagues; a prominent field for professional networks and social media.[31] *Fourthly*, the data – objective data and preferences – which HM delivers do not necessary provide all the information needed for personalizing data exploitation strategies, commercial practices, and standard terms. The missing elements are completed through proxies. The degree to which companies use proxies is subject to their

---

28 For an attempt to link the threefold distinction to the appropriate set of substantive rules, as well as rights, remedies and procedures, see H.-W. Micklitz, *The Politics of Justice in European Private Law*, n. 7, 283.

29 P. Hacker, Personalised Law and Behavioural Sciences, in C. Busch and A. De Franceschi (eds.), *Data Economy and Algorithmic Regulation, A Handbook* (Hart Publishing, 2020), forthcoming.

30 R. W. Reinsch, S. Goltz, M. Bakpayev, Appropriation of Likeness and Informed Consent in the Age of Surveillance Capitalism, Manuscript on file with the author.

31 S. Barocas and K. Levy, Privacy Dependencies, 95 *Washington Law Review* 555 (2020), available at https://ssrn.com/abstract=3447384, who also discuss proxies – our similarities and differences to others.

trade secrets and therefore difficult to quantify and to qualify.[32] The better the proxies, the less information is needed about individual preferences. Proxies add to the alter ego an alien element in that proxies replace the individual through standardized information. Whether and to what extent individual data on 'us' become superfluous and can be substituted to proxies is already subject to serious debate.[33]

c) The legal qualification of the alter ego

(25) The question is how to categorise the composite alter ego in between standardisation and individualisation. Those disciplines that dig deeper into transformation through digitization suggest understanding the 'person as commodity'[34] or 'the person as a product'.[35] The individual is replaced by their digitalized alter ego, which is a commodified digitalised person. Personalisation through AI would then abolish individualisation rather than realizing individualisation. Thus, personalisation is a misnomer: it insinuates the idea that personalisation may lead to individualisation, whereas it puts an end to individualisation and substitutes the individual through their alter ego. That is why the alter ego breaks down the distinction between individualisation and standardisation.

(26) In terms of remedies, the individual has standing to sue in regard to their alter ego. At the same time, treating the person as a commodity or as a product de-individualises them through standardisation techniques and justifies control of personalisation strategies through collective remedies. Collective entities have standing to sue the pre-designed so-called individualized personalisation techniques which allow construction of alter egos. The concept of pre-designed individual practices may serve as a starter.

d) Excursus - Shielding the individual personality against personalisation

(27) Is there a need to shield the individual personality against data-driven personalisation, against a process driven by private actors rather than the law,[36] not to mention the political economy of AI and machine learning?[37] Who is the addressee – business but also the

---

32 In 2020, H.-W. Micklitz has interviewed McKinsey and marketing research institutions.

33 As a consequence of the limits of the legal and practical limits of consent, see B. Custers, F. Dechesne, W. Pieters, B. Schermer and S. van der Hof, 'Consent and Privacy', in A. Schaber and A.T. Müller (eds), *The Routledge Handbook on the Ethics of Consent* (Routledge, 2018), 247 ff.; B. Custers, Click here to consent forever: Expiry dates for informed consent, *Big Data and Society* 2016, 1.

34 Using the now again fashionalbe language of K. Polanyi, *The Great Transformation* (Farrar & Rinehart, 1944).

35 More clearly as an algorithm, see Y. N. Harari, *Homo Deus, A Brief History of Tomorrow* (Harvill Secker, 2016), to paraphrise R. Romano, Law as a Product, Some Considerations of the Incorporation Puzzle, *Journal of Law, Economics and Organisation* 1985, 225 ff.

36 But who personalizes is all too often forgotten, see A. Verstein, Privatising Personalised Law, 68 *University of Chicago Law Review* (2019), 551 ff.

37 Y. Benkler, The Role of Technology in Political Economy, *Law and Political Economy* 2018, https://lpeblog.org/author/ybenkler.

consumer themselves? Philosophy discusses the implications of the gap between the individual personality and the alter ego. There is a need to distinguish between the alter ego created by business and the alter ego created by the consumer. The first variation has already become reality in discussion on whether consumers should be allowed access to their credit score so as to be able to improve relevant parameters, which is possible in the USA but impossible in Germany, as the consumer does not get to know the parameters.[38] What consumers and consumer organisations might understand as fair has a dark side – the temptation to adjust one's individual personality to one's alter ego. The second variation is more far reaching and well-known from social media, from computer games such as Second Life and from customization techniques. Consumers are invited to create a virtual if not an augmented reality, in which they can shape their alter ego.[39] If these data on the self-made alter ego are retrieved for whatever marketing purpose, then 'personalisation' might no longer be connected to existing individual preferences or those of their proxies but to virtual preferences. Who should be protected – the individual personality, the alter ego of the individual personality, or the virtually created alter ego, against what, by whom and what for? In light of the uncertainties over who is who, one might feel tempted to argue that virtual personalisation puts an end to personalised marketing techniques. The data retrieved are useless, because there is no individual which could be targeted. But what if the individual personality follows their virtual alter ego and thereby virtual preferences?

4. Techniques of personalizing marketing practices

(28) Abundant literature in marketing deals with all sorts of personalisation techniques. Business understands personalisation as an extremely efficient way to connect the consumer to a product and to avoid sunk costs. In light of the rather loose language in marketing, Strycharz, Noort, Helberger and Smit have not only provided a definition of personalisation but have identified *'seven techniques of personalising marketing messages'*. Their findings are based on interviews with practitioners, who claim that online players are the best at personalisation, the travel sector being on top and the gambling sector being close. Covid-19 might have changed the ranking. Strycharz, Noort, Helberger and Smit's classification highlights the conceptual confusion on personalisation vs. individualisation. More importantly it serves as a perfect starter for connecting personalisation to the technological infrastructure that lies at the core of digital asymmetry and later on to dark patterns, which

---

38 Just in parenthesis it should be recalled that Fintechs are testing other means than collecting data on credit history, such as the way in which consumers communicate in social media.

39 For a short introduction, see L. Reisch, S. Bietz and H.-W. Micklitz, *Algorithmen und Verbraucher* (Zeppelin Universität, Forschungszentrum Verbraucher, Markt und Politik, 2020), 65 ff., for a much deeper analysis of the key role of computer games for the transformation of legal concepts, see P. Palka, *Virtual property, towards a general theory* (ph.d. EUI, Florence, 2017), https://cadmus.eui.eu/handle/1814/49664.

provide a preliminary understanding of the kind of data exploitation strategies which are supposed to be unlawful.

(29) In the following we summarise the seven techniques,[40] which we will link to the distinction between individualisation and personalisation, the true individual personality and the digital alter ego. This categorisation indicates a huge knowledge gap between what companies are achieving through personalisation techniques and what consumers can find out about how their objective data are used as well as what their alter ego in the internet looks like. Due to the de-individualised alter ego, not much gain is to be had in granting consumers individual rights of disclosure. Even more important are collective disclosure rights which all aim to examine the lawfulness of personalisation techniques. In this respect we refer to Area 1.[41]

Category	Definition	Personalisation/individualisation
Online behavioural targeting	Adjusting advertisements to previous online behaviour, detected cookies and social media. 'Automated personalisation' matching product ID with consumer profile ID	Behavioural preference alter ego reconnectable to the individual at any time
Email marketing	Personalised name and content, focus on behaviour rather than content	Preferences (alter ego) more important than substantive individualisable information
Social media advertising	Major advantage: new types of public data and metadata, tags, comments and explicit personal relationships. Personalised advertising = targeting – lookalikes	Very high degree of individualisable data on individual personality, either directly or through social ties ('tell me who your friends are...')
Apps and notifications	Distinction between in-app and notifications, the former being more accepted whereas the latter raises resistance	If individualisable, the difference in behaviour offers potential for micro-targeting to overcome resistance
On-site personalisation	Website morphing relates to latent customer segments from clickstreams and changing the websites' look to maximise revenue	Personalisation through maximising behavioural preferences throughout,
Customisation	Freely choose own parameters and filters to develop own profile, personalisation is self-driven	Invitation to active alter ego-building through the consumer
Price differentiation	Differentiating online price for identical products/services based on information about potential customer	Indicating behavioural preferences and social status in the case of e.g. unknown behaviour

40 Strycharz, v. Noort, Helberger and Smit, n. 27, 643 f.

41 Helberger, Micklitz, Sax and Strycharz, n. 2, 3.10.

(30) What is the knowledge gain with a view to deciding over the legality of the seven techniques of personalisation? First and foremost it has to be recalled that the techniques are all lawful, at least as long as retrieval of personal data matches the requirements of the GDPR. The marketing industry is using the opportunities that 'free flow of personal data' within the Internal Market offers. However, the distinction between personalisation and individualisation ties in. As a formula one might conclude that personalisation becomes more problematic the more it is individualisable. This does not mean that personalisation does not cause problems. In fact the reason why personalisation is understood as a problematic data exploitation strategy is that the consumer has no chance to understand the power structure that stands behind retrieval and processing of data. As explained in the Area 1 study,[42] a marketing company may avoid the legal trap if it is in a position to show that collecting and processing of personal data is fully in line with the European legal framework. However, connecting personalised behavioural preferences to the individual casts increasing doubt on marketing strategies. This is particularly true when commercial practices aim to exploit individual and/or personal situational vulnerabilities. In theory each of the seven techniques could be used in such a way. This is what the third column is meant to demonstrate.

(31) Digitization is moving. In their survey, Strycharz, Noort, Helberger and Smit do not touch upon what Clifford termed 'The Monetisation of Online Emotions'.[43] The future might be that consumers'[44] emotions are being detected in real time and tracked, both in public and private spaces.[45] New computational means facilitate micro-targeting of the *individual* personality and adaptation of market offers accordingly, in potentially manipulative ways.[46] The reason why the practitioners interviewed might not have referred to emotional marketing strategies might simply be that the technology needed was not yet at a stage where marketers can easily use it. This may soon change. Exploitation of our emotions through personalised marketing techniques is meeting strong resistance. One might even discuss the need to shield the individual personality against emotional AI marketing techniques. Due to the constitutional dimension behind the scope and reach of fundamental rights, the search for a solution does not lie in the hands of the EU alone.

---

42 ibid.

43 D. Clifford, *The Legal Limits to the Monetisation of Online Emotions* (ph.d., KU Leuven, 2019, id., EU Data Protection Law and Targeting Advertising, Consent and the Cookie Monster – Tracking the crumbs of online user behaviour, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 2014, 194.

44 P. Hacker, Manipulation by Algorithms, Exploring the Triangle of Unfair Commercial Practices, Data Protection and Privacy law, Working Paper, August 2020, on file with the author.

45 P. Valcke, D. Clifford and V.K. Steponaité, Constitutional Challenges in the Emotional AI Area, in H.-W. Micklitz, O. Pollincino, A. Simoncini, G. Sartor and G. De Gregorio (eds.), *Constitutional Challenges in the Algorithmic Society* (Cambridge University Press, 2021), forthcoming.

46 Hacker, n. 4, 266, Q. Weinzierl, Dark Patterns als Herausforderung für das Recht, Rechtlicher Schutz vor der Ausnutzung von Verhaltensanomalien, *Neue Zeitschrift für Verwaltungsrecht - Extra* 2020, 1 ff.

5. *Personalisation and dark patterns*

(32) Personal data can be used for good and for bad: for good in that data are used to provide the consumer with personalised information which they appreciate as a form of orientation, for instance on books that touch upon the consumer's preferences, or for offering better prices to the economically vulnerable (!); for bad through all sorts of unfair commercial practices, which cause or exploit[47] not (only) external structural but (also) internal situational vulnerabilities.[48] The catchphrase for these techniques is 'dark patterns'. Connecting personalisation and dark patterns requires clarification about what is understood by dark patterns, how dark patterns fit into the concept of external and situational digital vulnerability and digital asymmetry, whether and how dark patterns can be personalised and whether and under what conditions (personalised) dark patterns can be classified as *per se* unlawful.

(33) This is how dark patterns are commonly circumscribed:[49]

> The term "Dark Patterns" refers to unfair techniques and tricks that mislead consumers in the use of websites and apps and induce them to give unwanted consent or perform unwanted actions. Learned behavioural patterns are manipulated in a targeted manner by cleverly placed buttons or drop-down menus. Fast scrolling and browsing through websites or apps might then lead to wrong assumptions. A wrongly placed check mark, an option hidden in a drop-down menu or simply information printed in very small print allows unwanted newsletter subscriptions, paid registrations or goods and services that have been smuggled secretly into the shopping cart. The web designer Harry Brignull coined the term. On the website www.darkpatterns.org and the Twitter account @darkpatterns, corresponding practices are collected.

(34) Today, dark patterns are also referred to as a targeted form of so-called "sludges",[50] which discriminate against rather than support consumers, sometimes also called dark nudges.[51] Under reference to Bogenstahl and Mathur et al., Reisch and Bietz[52] have produced an overview of dark patterns, a list which needs to be constantly modified and updated (see

---

47 For a broader discussion of causing vulnerabilities and exploiting vulnerabilities, see Palka, n. 21.

48 The distinction between external structural and internal situational vulnerability is explained and defined in Helberger, Micklitz, Sax and Strycharz, n. 2.

49 Based on Reisch, Bietz and Micklitz, n. 39, 10 ff; see also Weinzierl, n. 46, 1 with extensive references

50 C.R. Sunstein, Sludge audits, *Behavioural Public Policy* 2020, 1 ff.

51 L.A. Reisch, Nudging hell und dunkel: Regeln für digitales Nudging. *Wirtschaftsdienst* 2020, 87 ff.

52 See Reisch, Bietz and Micklitz, n. 39, 10 f., under reference to C. Bogenstahl, *Dark Patterns –Mechanismen (be)trügerischen Internetdesigns* (Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB). 2019), https://www.tab-beim-bundestag.de/de/pdf/publikationen/themenprofile/Themenkurzprofil-030.pdf; A. Mathur, G. Acar, M.J. Friedman, E. Lucherini, J. Mayer, M. Chetty and A. Narayanan, Dark patterns at scale: Findings from a crawl of 11K shopping websites. In *Proceedings ACM Human-Computer Interaction* (Vol. 3, 2019, Art. 81). https://doi.org/10.1145/3359183. L. Reisch and S. Bietz have put together the facts that served me as the basis of the legal analysis.

below). Whilst containing at least partly new wine in old bottles, the list serves as a wonderful starter to clarify the link between dark patterns and personalisation.

(35) Three clarifications are needed in order to properly place the definition into the context of our analysis. First and foremost the category of misleading dark patterns does not apply to the ground level of digital exploitation strategies. Information in whatever form and however correct it might be is not suited to overcoming the external structural power imbalance at the ground level. Misleading dark patterns may, however, gain importance at the surface level when it comes to the question of how the data exploitation strategy is communicated. A case in point is the newly introduced obligation to inform the consumer of personalised prices (see below). Secondly, dark patterns cover two different forms of data exploitation strategies. The first is how companies might develop strategies to gain access to personal data so as to be able to collect them; the second refers to data processing, of the kind of algorithms that are used to exploit collected data to the greatest benefit of business. Thirdly, those who work with dark patterns put emphasis on the subjective side. 'Misled', 'unwanted', 'manipulated', 'hidden' insinuates 'intention' on the part of marketers who aim to build a digital infrastructure that exploits consumers. Whilst this might occasionally be true, putting emphasis on the subjective dimension could easily lead into a dead-end street. Usually the burden of proof is on the person or institution who claims that an infringement has been committed 'intentionally'. The law on unfair commercial practices, however, does not require any negligence; it grew out of tort law and from there into a market clearance mechanism. But there is more. Stressing intentionality and thereby 'guilt' triggers a wrong debate. The consumer does not need to be the target of an intentionally committed dark pattern in order to trigger the scope of application of the UCPD, GDPR or UCTD. It suffices that the consumer suffers from structural and universal digital vulnerability so as to trigger a reversal of the burden of proof. Dark patterns are the result of a specifically designed digital architecture. That is why the study by the Norwegian Consumer Council bears the telling title 'Deceived by Design'[53] and that is why Willis speaks of 'Deception by Design.[54] Consumers cannot escape dark patterns.[55]

(36) Personalisation adds a third layer to gaining access to personal data and to processing data in the most profitable way. Personalisation lifts the use of data exploitation strategies to a new level. It is a matter of definition whether one understands personalisation as a third layer or as a strategy that cuts across collection and processing. What really matters is that

---

53 Norwegian Consumer Council, *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy* (Norwegian Consumer Council, 2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

54 L. Willis, Deception by Design, *Legal Studies Paper No. 2020-25* (2020).

55 L. Smith, *Why you can't escape dark patters*, https://www.fastcompany.com/90452333/why-you-still-cant-escape-dark-patterns.

thanks to big data and big data analytics the marketing industry is now in a position to target personalised and individualised preferences, which means personalisable groups/categories of consumers if not individualisable consumers directly. Connecting an established set of dark patterns to personalisation demonstrates how an already problematic strategy can be turned into an even more powerful tool to exploit personal/individual situational vulnerabilities.

Category	Definition	Personalisation (P)
Trick questions	When filling out forms, ambiguous questions are asked to get answers that users had not intended	P allows establishing on whom the trick works and does not work
Sneak into Basket	While shopping on the Internet, additional items are added to the shopping cart, often through preset options on previous pages	P allows detection of those consumers who can easily be trapped
Roach Motel	Easy to take out premium subscriptions, cancelling them again is made much more difficult	The model is old, P allows targeting those who invest in the search to cancel and those who do not
Privacy Zuckering	Extraction techniques: how one is tempted to share more personal data publicly than intended	P allows distinguishing between those where the technique works and where it does not work
Price Comparisons Prevention	Rendering price comparison between items difficult	An old strategy, P allows detection of who can easily be trapped
Misdirection	Design directs attention to one thing in order to distract from another e.g. mandatory information	P allows distinguishing between those where the design works and where it does not
Hidden Costs	Only in the last step of the order process are unexpected costs such as shipping charges, taxes or fees displayed	An old strategy, special consumer protection rules in place P allows establishing when the strategy works and on whom
Bait and Switch	During a certain process something completely different happens, so as to surprise consumers	An old strategy, special consumer protection rules in place UCPD annex 1 lit 5 P allows establishing who can easily be caught by surprise
Camouflaged Advertising	Advertisements disguised as navigation points or other content	P allows establishing when and on whom the strategy works
Disguised Ads	Free trial version converted into paid services; credit card is charged tacitly	Special consumer protection rules in place (button solution) P allows establishing where the strategy works, who complains and who does not complain

Confirm Shaming	Refusal formulated so that consumers feel guilty if they refuse	Example of emotional AI P allows targeting of those who easily feel guilty
Friends Spam	Under pretext, email or social media accesses are queried; then spam is sent in the name of the user	Prima facie no P Potentially differentiate between those who have many friends where the strategy might be particularly useful

(37) Tentatively and based on the forgoing analysis, three hypotheses can be formulated. Firstly, personalisation may serve as a technique to render old and well-known marketing strategies much more efficient and even to circumvent existing consumer protection rules by targeting situational vulnerabilities. Secondly, personalisation allows use of the new opportunities offered by big data and big data analytics to differentiate between those consumers who can easily be trapped and those who are able to avoid the new techniques. Thirdly – and this is more a conclusion than a hypothesis – personalisation allows targeting vulnerabilities and then exploiting them accordingly.

(38) This brief overview on the potential of personalised dark patterns offers two additional insights. Firstly, the consumer is unable to uncover the technological infrastructure that stands behind personalised marketing techniques, let alone the reasons why they are being targeted. And secondly, the enforcement authorities, whether public or private, have a mountain to climb in order to decipher the technological infrastructure and then to distil out of the technological infrastructure potential strategies which are built on exploitation of vulnerabilities.

6. Mismatch

(39) In the following we will apply the legal control architecture, characterised through the interplay between judicial review of standardised and individual data privacy policies, commercial practices and standard terms, as well as a common denominator of fairness to personalised commercial practices and personalised prices. It will have to be shown that a substantial mismatch exists between the potential of legal control architecture to get to grips with personalisation, on the one hand, and the foreseeable results on the other. The EU legislature legalises personalisation subject to easily satisfiable requirements, leaving control of potential misuses to the enforcement authorities, the administration and the courts, who are in charge of providing the necessary evidence.

(40) We will first analyse personalised pricing as the EU has most recently introduced information requirements to the benefit of consumers before we turn to a deeper analysis of personalised commercial practices. The focus is led on consumer law, unfair commercial practices and non-discrimination law. As the EU data protection framework draws no meaningful distinction between personalised pricing and more general personalisation

practices, the extent to which such personalisation complies with the GDPR will be considered below.

II. Personalised pricing

(41) Personalised pricing can be described as price differentiation for identical products or services at the same time based on information a company holds about a potential customer.[56] In our context, personalisation is best understood as a pre-designed form of quasi-individualised standardisation in the sense that the outcome of the personalisation process may be individualised but the process by which the outcome is achieved is standardised by using algorithms. The use of such techniques is understood as a matter of collective interest and is to be challenged by collective mechanisms as we will show in the following. In terms of retrieval of data, such data exploitation strategies affect the ground level, whereas the way in which price personalisation is communicated relates to the surface level. This distinction between ground and surface levels explains why disclosure of personalised pricing is of limited value in the fight against digital asymmetry.

1. Economics of personalised pricing

(42) Personalised pricing serves to adjust the price to the willingness to pay of heterogeneous customers in order to maximise profits. This of course presupposes in-depth knowledge of the targeted consumer. Thereby, the trader can try to increase profits by charging higher prices to personalised customers or by acquiring new customers (through lower prices) that would otherwise not purchase the product or service.[57] This type of price personalisation is often called 'first degree price discrimination', whereas 'second degree price discrimination' relates to different prices for different qualities or quantities sold to the same buyer, which includes loyalty schemes. Finally, 'third degree price discrimination' means selling the same goods to different groups of customers at different prices. This would include student discounts, need-based tuition scholarships or 'ladies' nights'.[58] Empirical studies have demonstrated that traders applying first degree price discrimination have increased profits by up to 34 % as compared to a uniform price strategy.[59]

---

56 See, e.g., J. Poort and F.J. Zuiderveen Borgesius, Does everyone have a price? Understanding people's attitude towards online and offline price discrimination, *Internet Policy Review* 8 (2019), 1.

57 ibid., 4.

58 On the three degrees of price discrimination, see A.A. Miller, What do we worry about when we worry about price differentiation, *Journal of Technology Law and Policy* 19 (2014), 41, 55.

59 See R. Kahn and D.J. Jain, An Empirical Analysis of Price Discrimination Mechanisms and Retailer Profitability, *Journal of Marketing Research* 42 (2005), 516 ff.

(43) In terms of individual consequences, consumers can clearly benefit from personalised pricing where prices are lowered to match their willingness to pay, whereas others will pay more than the average price. In that sense, some authors have attributed to personalised pricing a distributive effect in that poorer consumers are charged less than wealthy consumers.[60] However, it should be noted that income is by no means the only factor that is taken into account; indeed, there has also been evidence of price differentiation that favours high-income areas. Moreover, as no average prices are indicated,[61] it is impossible to know which consumers benefit.

(44) In terms of welfare effects, personalised pricing can turn out in different ways.[62] Where the trader extends its business, thereby recovering fixed costs, and low-spending consumers obtain a product or service at a price below the otherwise applicable equal price level that they could not have afforded otherwise, both sides benefit from personalised pricing, and total welfare increases. Otherwise, where the trader simply exploits individual willingness to pay without extending its business, trader surplus will be realised at the expense of consumer surplus.[63] This strategy can even lead to a net welfare loss when producers gain but consumers lose more.[64]

(45) Finally, both sides can lose, due to competition effects, as consumers may be disappointed with the personalisation strategy and turn to other offers in the market.[65] Thus personalisation may even lead to general welfare loss. Finally, one would have to consider that price personalisation creates transaction costs for traders by way of investment in IT and/or the acquisition of data which must be recovered through the price of goods and services,[66] and even more for consumers (that are informed about the existence of price differentiation strategies) who need to spend more time on discovering such strategies and/or influencing their scores, which increases their search costs.

---

60 See E.I. Obergfell, Personalisierte Preise im Lebensmittelhandel - Vertragsfreiheit oder Kundenbetrug?, *Zeitschrift für* Lebensmittelrecht 2017, 290, 294; D. Tietjen and B.F. Flöter, Dynamische und personalisierte Preise: Welche lauterkeitsrechtlichen Schranken gelten für Unternehmen?, *Praxis im Immaterialgüter- und Wettbewerbsrecht* 2017, 546, 548; S. Genth, Dynamische Preise: ein Gewinn für Handel und Verbraucher, *Wirtschaftsdienst* 2016, 863.

61 This has been a political claim by the Consumer Centre of Northrhine-Westphalia, see Verbraucherzentrale Nordrhein-Westfalen*, Verbraucherproblemen wirksam begegnen – Weichen richtig stellen*, 2017,

https://www.verbraucherzentrale.nrw/sites/default/files/migration_files/media247515A.pdf

62 For an overview, see F.J. Zuiderveen Borgesius and J. Poort, Online Price Discrimination and EU Data Privacy Law, *Journal of Consumer Policy* 40 (2017), 347, 353 f.

63 Consumer surplus happens when the price that consumers pay for a product or service is less than the price they are willing to pay.

64 See also T.J. Tillmann and V. Vogt, Personalisierte Preise im Big-Data-Zeitalter, *Verbraucher und Recht* 2018, 447, 448 f.

65 See, e.g., P. Kenning and M. Pohst*,* Die verbraucherwissenschaftliche Perspektive: von der Customer Confusion zur Price Confusion?, *Wirtschaftsdienst* 2016, 871, 872.

66 See H. Zander-Hayat, L.A. Reisch and C. Steffen, Personalisierte Preise – Eine verbraucherpolitische Einordnung, *Verbraucher und Recht* 2016, 403, 406.

(46) Overall, the economics of personalised pricing certainly do not indicate that consumers benefit from it, rather to the contrary; which is not least an issue in competition law (see below on competition law). Moreover, it brings new ground for market failure with it. Due to the opacity of prices, one of the most important criteria for the consumer's purchasing decision is obscured. Price comparison tools, which the EU legislator in particular views as a great help for consumers,[67] fail as well if they cannot reflect the personalised price that the individual user of that tool is offered.

2. *Consumer perceptions of personalised pricing*

(47) As mentioned above, personalised pricing would normally be beneficial to some consumers, while others would have to pay higher prices as compared with a uniform price strategy. Thus, those who are offered cheaper prices, due to their limited willingness (or ability) to pay, could be expected to be positive about personalised pricing, whereas those who would have to pay more should be opposed to personalised pricing. However, consumer polls[68] as well as expert studies have shown that the majority of consumers regard personalised pricing as unfair.[69] This includes consumers who expect to benefit from that strategy, [70] although the share of those who think positively about personalised pricing is of course higher among those that are confident of making a good deal.

(48) A study by Reinatz et al [71] has revealed that consumers' attitudes towards personalised pricing depend on several factors. For example, if the sales situations differ, consumers do not tend to think about price differentiation but about different offers. Acceptance of different prices is greater where a better price is achieved by one's own efforts, such as intensive search. Here, control is an important factor: Are there certain price rules that the consumer can adjust to, such as regularity of certain petrol price levels at certain times of the day?

(49) Moreover, certain price differentiations are generally accepted as fair, such as cheaper tickets for children or the elderly (third degree price discrimination). Finally, the motivation of the trader matters: Does it have a 'good reason', such as passing on prices it has to pay

---

67 See recital (22) Payment Accounts Directive 2014/92/EU: 'Comparison websites that are independent are an effective means for consumers to assess the merits of different payment account offers in one place. Such websites can provide the right balance between the need for information to be clear and concise and the need for it to be complete and comprehensive, by enabling users to obtain more detailed information where this is of interest to them. (...).'.

68 ibid., 407, with further references.

69 For a theoretical foundation, see Miller, n. 58, 84 ff.

70 See W. Reinartz et al., *Preisdifferenzierung und –dispersion im Handel* (IFH-Förderer, 2017), 3; W. Reinartz and N. Weigand, Die Gefahren der Preisdifferenzierung im Einzelhandel: Warum niemand gewinnt, wenn Kunden draufzahlen, *NIM Marketing Intelligence Review* 2019, 31 ff.

71 See Reinartz et al., n. 70.

itself, or does it simply wish to maximise profits?[72] A study by Harris Interactive has produced similar results.[73]

(50) Similarly, a study by Poort and Zuiderveen Borgesius[74] found that a large majority of Dutch consumers would favour prohibition of personalised pricing, and that more than 80% of consumers found price discrimination to some extent unacceptable and unfair. Again, this included even those consumers who benefit from price discrimination. Almost 80% thought that traders should have to lay open price discrimination strategies. And again, the basis for price personalisation has a great influence on consumers' reactions.[75] Whereas loyalty cards, student discounts and quantity discounts (second and third degree price discrimination) were generally accepted, price differentiation related to use of a particular device (first degree price discrimination) was regarded as most unacceptable. Opacity of price strategy leads to objection.[76]

(51) In terms of personalised pricing on the internet, all factors seem to turn against consumer acceptance. It is the same situation for everybody, in that the rules of price determination are unknown and therefore beyond the consumer's control, while the consumer – if aware of price personalisation – will certainly assume that it is motivated by profit maximisation.

(52) The empirical findings appear to be confirmed by public reactions to previous incidents of personalised pricing. When Amazon personalised pricing in 2000 (claiming this only to have been an experiment), the public outcry was such that Amazon stopped the attempt immediately.[77] The same happened when Orbitz was discovered to be steering Mac OS X users towards more expensive hotels in select locations by placing them in higher ranks in search results.[78] Ever since, traders have shied away from personalising prices openly but use 'fencing' strategies to conceal them.[79]

---

72 ibid., 3

73 See Harris Interactive, *Dynamisches und indviduelles Pricing*, https://harris-interactive.de/opinion_polls/dynamisches-und-individuelles-pricing.

74 Poort and Zuiderveen Borgesius, n. 56, 6 ff.

75 ibid., 10 ff.

76 On the latter, see also M. Schleusener and S. Hosell, *Personalisierte Preisdifferenzierung im Online-Handel* (SVRV, 2016), 13 f.

77 ibid., 2.

78 See A. Hannak et al., *Measuring Price Discrimination and Steering on E-commerce Web Sites*, http://conferences.sigcomm.org/imc/2014/papers/p305.pdf, 2014, 1.

79 See M. Zhang and P. Bell, Price Fencing in the Practice of Revenue Management: An Overview and Taxonomy, 11 *Journal of Revenue and Pricing Management* (2012), 146 ff. See also Zuiderveen Borgesius and Poort, n. 62, 349 f.

3. *The current EU legal framework*

(53) As a preliminary remark, one has to note that EU law has not yet dealt comprehensively with personalised pricing. In particular, EU law does not take into account the digital asymmetry between traders and consumers that we unfolded above. Rather, it seems to be guided by a flawed understanding of freedom of contract that fails to take into account that freedom of contract involves fully informed decision-making *on both sides*. Moreover, consumer protection law is characterised by the complete separation of the law relating to collection and processing of personal data, its acquisition from third parties, and its use for personalisation of prices. Only considering the last step, personalisation of prices neglects the potentially questionable origin of the data (the ground level) as well as questions as to what the consumer has really consented to, to whom they have consented, or whether consent was perhaps invalid, or held invalid even years later in collective proceedings brought under the UCTD.

a) Freedom of Contract

(54) At first glance, exploitation by way of personalised pricing seems to be in line with the principle of freedom of contract. This principle is fundamental not only to the civil law orders of Member States but also to EU private law[80] in general[81] and under Article 16 Charter of Fundamental Rights in particular.[82] Thus, in principle, everybody is free to contract, or not to contract, with other persons under conditions that the parties choose to apply to their contract. In relation to price increases and decreases, the *Bundesgerichtshof* (Federal Supreme Court) held in 2003 that the trader is free in its decision on price. It can increase or decrease its publicly announced prices at any time as it finds suitable, as long as this is not in breach of price laws and as long as the circumstances do not suggest an unfair commercial practice. Such circumstances include the situation where price increases and decreases are used to disguise the 'real price' and make a sky-high price appear reasonable.[83] In a decision of 1958, the *Bundesgerichtshof* held that freedom of contract included the right to charge different customers different prices, unless special aggravating circumstances are in place.[84]

---

80 See J. Basedow, Freedom of Contract in the European Union, *European Review of Private Law* 2008, 901 ff.

81 See ECJ, 16/1/1979, Case 151/78 *Sukkerfabriken Nykøbing Limiteret* v. *Ministry of Agriculture*, ECLI:EU:C:1979:4, para. 20; ECJ, 5(10/1999, Case C-240/97 *Spain* v. *Commission*, ECLI:EU:C:1999:479, para. 99. It was pointed out, however, that freedom of contract was weaker in European private law than in national private laws, see B. Heiderhoff, Vertrauen versus Vertragsfreiheit im europäischen Verbrauchervertragsrecht, *Zeitschrift für Europäisches Privatrecht* 2003, 769 ff.

82 See the Explanations Relating to the Charter of Fundamental Rights, OJ 2007 C 303/17, Explanation on Article 16 – Freedom to conduct a business, and ECJ, 22/1/2013, Case C-283/11 *Sky Österreich GmbH* v. *Österreichischer Rundfunk*, ECLI:EU:C:2013:28, para. 42; ECJ, 18/7/2013, Case C-426/11 *Mark Alemo-Herron and others* v. *Parkwood Leisure Ltd*, ECLI:EU:C:2013:521, para. 32.

83 See BGH, 13/3/2003, I ZR 212/00, *Neue Juristische Wochenschrift* 2003, 2096.

84 See BGH, 18/4/1958, I ZR 158/56, *Gewerblicher Rechtsschutz und Urheberrecht* 1958, 487.

Indeed, such aggravating circumstances might be seen in the fact that personalisation is performed by algorithms on a nontransparent factual basis and using a nontransparent calculation method, which leaves the consumer in the dark about price logic. This is exactly the situation which mirrors the consumers' digital vulnerability, here translated into digital asymmetry.

(55) Freedom of contract may of course be limited so as to balance it with competing fundamental rights and with the public interest.[85] Indeed, freedom of contract has been limited in relation to personalised prices in various ways. It must not be applied in breach of antidiscrimination law, and according to a new information obligation in the Consumer Rights Directive 2011/83/EU, as amended by the Omnibus Directive (EU) 2019/2161, the trader must lay open that it applies personalised pricing.

b) Antidiscrimination law

(56) The overall framework of anti-discrimination law with regard to fairness and the distinction between standardisation/individualisation and collective vs. individual remedies has already been explained. Here, the focus is on anti-discrimination law and price discrimination.

(57) Discrimination in relation to the supply of goods and services is dealt with by Directive 2000/43/EC implementing the principle of equal treatment between persons irrespective of racial or ethnic origin[86] and by Directive 2004/113/EC implementing the principle of equal treatment between men and women in access to and supply of goods and services.[87] National legislators may have extended the prohibition of discrimination to other reasons. For example, the German legislator has extended the principle of equal treatment to religion, disability, age and sexual identity.[88] Clearly, this also applies where discrimination is hidden in an algorithm,[89] although the GDPR has not taken up this issue.[90]

(58) Potential remedies under EU anti-discrimination law are injunctions and damages.[91] Moreover, the use of discriminatory personalised prices may constitute an unfair

---

85 See, e.g., ECJ, 6/9/2012, Case C-544/18 *Deutsches Weintor eG* v. *Land Rheinland-Pfalz*, ECLI:EU:C:2012:526, paras 47 and 54; CJEU, *Sky Österreich*, n. 82, para. 46.

86 [2000] OJ L 180/22, in particular Art 3(1)(h).

87 [2004] OJ L 373/37.

88 See § 19 para. 1 *Allgemeines Gleichbehandlungsgesetz* (General Act on Equal Treatment; AGG).

89 See Genth, n. 60, 866; SVRV, *Verbrauchergerechtes Socring* (SVRV, 2018), 135 ff.; Hacker, n. 5.

90 Only recital (71) GDPR mentions the risk of discriminatory profiling, see P. Scholz, DSVGO Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling, in S. Simitis, G. Hornung and I. Spiecker (eds), *Datenschutzrecht* (Nomos, 2018), para. 14.

91 With regard to the overall control architecture, see above. Whether or not the victim can also claim conclusion of the desired contract is discussed controversially, see G. Thüsing, AGG § 21 Ansprüche, in C. Schubert (ed), *Münchener Kommentar zum Bürgerlichen Gesetzbuch*, vol. 1, 8th edn (C.H. Beck, 2018), paras 17 ff., with further references.

commercial practice and can therefore be challenged in collective actions.[92] However, according to German case law, anti-discrimination law does not apply to the relationship between a credit rating agency and a consumer, as the credit rating agency does not supply goods or services to the consumer but is only a third party, despite its influence on the actual supply or service relationship with a trader.[93] Thus, a consumer cannot successfully challenge the origin of a discriminatory score but only its use by individual traders. This reduces the effectiveness of anti-discrimination law, in particular when compared to unfair contract terms law where consumer organisations can challenge the recommendation of an unfair term, for example, by a business organisation, so as to avoid its being spread.

(59) The crucial issue will lie in detection and proof of discrimination.[94] Generally speaking, the burden of proof lies with the claimant, although EU law prescribes reversal of the burden of proof in situations where the potential discrimination victim provides facts from which it may be presumed that direct or indirect discrimination has occurred.[95] However, according to the leading opinion of anti-discrimination lawyers, reversal of the burden of proof only relates to causation between the special characteristics of the potential victim (for example, religion) and the different treatment. The consumer must still prove the different treatment as such, and they have no claim related to information from the trader on how it treated other consumers,[96] or what the score would be if, for example, a female claimant was male.[97] As explained in the Area 1 study,[98] digital asymmetry requires a change of this approach towards a comprehensive reversal of the burden of proof.

(60) One notable exception from anti-discrimination law is unequal treatment regarding credit. According to the German government, credit is not 'available to the public irrespective of the person concerned' in the terms of Article 3(1) of Directive 2004/113/EC and is therefore considered to be outside the scope of application of that Directive.[99]

---

92 For Germany, see D. Tietjen and B.F. Flöter, Dynamische und personalisierte Preise: Welche lauterkeitsrechtlichen Schranken gelten für Unternehmen?, *Praxis im Immaterialgüter- und Wettbewerbsrecht (GRUR-Prax)* 2017, 548.

93 See OLG Munich, 12/3/2014, 15 U 2395/13, *Zeitschrift für Datenschutz* 2014, 570, 572.

94 See also SVRV, Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt (SVRV, 2016), 70.

95 See Art. 8(1) Directive 2000/43/EC and Art 9(1) Directive 2004/113/EC.

96 For details, see G. Thüsing, AGG § 22 Beweislast, in Schubert, n. 91, paras 6 ff.

97 See OLG Munich, n. 93, 573.

98 Helberger, Micklitz, Sax and Strycharz, n. 2.

99 See the explanations of the German government on draft legislation to implement EU anti-discrimination law, *Bundestags-Drucksache* 16/1780, 42. For a different view on small credit, see G. Thüsing, AGG § 19 Zivilrechtliches Benachteiligungsverbot, in Schubert, n. 91, para. 25, for a broader discussion of 'publicness' see above.

c) Information on personalised pricing – the Consumer Rights Directive

(61) The so-called 'Omnibus' Directive (EU) 2019/2161 on better enforcement and modernisation of EU consumer protection rules[100] amended the Consumer Rights Directive 2011/83/EU by introducing, in Article 6(1)(ea), a new information obligation on traders, according to which they must inform the consumer, 'where applicable, that the price was personalised on the basis of automated decision making'. At the same time, recital (45) of Directive (EU) 2019/2161 confirms that '(t)raders may personalise the price of their offers for specific consumers or specific categories of consumers based on automated decision-making and profiling of consumer behaviour allowing traders to assess the consumer's purchasing power'.

(62) The legal consequences of a breach of that information obligation can be derived from the Consumer Rights Directive as well as from the Unfair Commercial Practices Directive 2005/29/EC, as implemented in the Member States. The Consumer Rights Directive, like basically all EU consumer legislation, calls for adequate and effective means to ensure compliance with the Directive, without specifying those means. Thus, Member States have a certain amount of discretion over how to sanction breaches, and there is no guarantee that a breach of the obligation to inform the consumer about personalised prices will impact on the validity of the contract.

(63) Article 23(2) Consumer Rights Directive calls for collective mechanisms by public bodies, consumer organisations and/or professional organisations. Until now, such measures have often failed to compensate affected consumers for losses; which is why the Injunctions Directive 2009/22/EC is being replaced by the new Directive (EU) 2020/1282 on representative actions that provides for mechanisms from which consumers can benefit directly. Finally, the Omnibus Directive has amended Article 24 Consumer Rights Directive on penalties by laying down non-exhaustive and indicative criteria that Member States should take into account when imposing penalties on traders, thereby strengthening public law enforcement of the Directive including the obligation to inform the consumer about personalisation of prices. It remains to be seen whether the amendment leads to a 'penalisation' of consumer law.

(64) At the same time, Article 7(5) Unfair Commercial Practices Directive links breach of an information duty under EU consumer law with unfair commercial practices law. Under Article 7(1) Unfair Commercial Practices Directive, '(a) commercial practice shall be regarded as misleading if, in its factual context, taking account of all its features and circumstances and the limitations of the communication medium, it omits *material* information that the average consumer needs, according to the context, to take an informed transactional

---

100 OJ 2019 L 328/7.

decision and thereby causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise.' Article 7(5) specifies that '(i)nformation requirements established by Community law in relation to commercial communication including advertising or marketing, a non-exhaustive list of which is contained in Annex II, shall be regarded as material.' The Consumer Rights Directive, like one of its predecessors, the Distance Selling Directive 97/7/EC, clearly belongs to EU law in relation to commercial communication that Article 7(5) refers to.

(65) Thus, the provisions of Directive 2005/29/EC on enforcement and penalties also apply to a breach of the obligation to inform the consumer about the application of personalised pricing. Under Article 11, this includes adequate and effective means to enforce compliance with the Directive, including collective action by public authorities and/or consumer organisations but also competitors, and Article 13 requires Member States to lay down effective, proportionate and dissuasive penalties for breaches of the Directive (as implemented), whereas again the Omnibus Directive added a second paragraph with non-exhaustive and indicative criteria that Member States should take into account when imposing penalties on traders.

(66) Importantly, with the Omnibus Directive a new Article 11a on 'Redress' was inserted in the Unfair Commercial Practices Directive. According to Article 11a(1), consumers harmed by unfair commercial practices shall have access to proportionate and effective remedies, including compensation for damage suffered and, where relevant, a price reduction or termination of the contract. Member States may determine the conditions for the application and effects of those remedies. They may take into account, where appropriate, the gravity and nature of the unfair commercial practice, the damage suffered by the consumer and other relevant circumstances. With all caution due to the discretion that Article 11a(1) leaves to Member States, this could be an important remedy that would allow consumers to cancel a contract where personalised pricing is unknown to the consumer. Instead, it would seem unlikely that consumers could ask for a reduction in the 'real price', as it will be excessively difficult to determine the 'real price' where traders apply personalised pricing. With the new redress action of Directive (EU) 2020/1828, these redress claims can also be enforced in collective actions brought by qualified entities.

(67) The new information obligation has some serious limitations, though. First of all, it only applies within the scope of application of the Consumer Rights Directive 2011/83/EU, from which a vast number of contracts are excluded, most importantly financial services contracts. A second limitation of probably little practical relevance relates to the notion of 'automated decision making'. Only where price personalisation occurs 'on the basis of automated decision making' does the trader need to make that practice transparent. The notion of automated decision-making is well-known from data protection law. According to

Article 22 GDPR,[101] a data subject shall not be subject to a decision based *solely* on automated processing, including profiling, which produces legal effects that – or otherwise similarly operates to – significantly affect them. The basic aim of this provision is related to human dignity and fundamental rights: the exercise of fundamental freedoms by human beings should not be subjected to the decision of an algorithm but a decision with legal effects should always be made by a natural person.[102]

(68) Usually, no human intervention will occur in an algorithm-driven price-setting process of an online trader. Moreover, it should be clear that not only does automated price-setting constitute an 'automated decision' but the same applies where an employee sets the price that was determined by an algorithm without adding their own thoughts. Only a new decision that takes other factors into account constitutes a relevant human intervention.[103] These principles apply to internal scores (calculated by the trader) as well as to external scores (calculated by a credit rating agency or by some other reputable service provider), as usually the trader will not collect all the pieces of information and process them itself into a credit score but rely on the credit score that a credit rating agency has calculated on the basis of the information it has available.[104]

(69) A third limitation that is of more importance is the content of the information obligation. The trader only has to lay open that it is applying personalised pricing but not what criteria it uses to do so, or how it weighs those criteria; a problem that is well-known from the debate on credit scores. Of course, the consumer could use their rights under the GDPR to find out what personal data the trader avails of and to assess whether they are correct in the first place. The consumer could also inquire about 'the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject', according to Article 13(2) lit. f) GDPR. All this is, however, totally unrealistic in a shopping situation. And even with that information, the consumer would not be able to understand whether ground level personalisation of prices is beneficial or detrimental to them but must take a decision under complete uncertainty. Shopping turns into gambling.

(70) Thus, the only use of information obligations can be seen in the consumer's possibility to avoid a particular trader. This possibility again has its limitations. First, avoiding a trader is

---

101 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, [2016] OJ L 119/1.

102 See Scholz, n. 90, para. 3.

103 See Scholz, n. 90, para. 29; M. Helfrich, DSVGO Automatisierte Entscheidungen im Einzelfall einschließlich Profiling, in G. Sydow (ed.), *Europäische Datenschutzgrundverordnung*, 2nd ed. (Nomos, 2018), paras 43 f.

104 See Scholz, n. 90, para. 29; against M. Martini, DS-GVO Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling, in B.P. Paal and D.A. Pauly (eds), *DS-GVO – BDSG*, 2nd ed. (C.H. Beck, 2018), para. 24.

not an option where the trader cannot be avoided because it performs an essential service – a situation discussed in a separate study.[105] Second, avoidance may no longer work in the future if personalisation of prices becomes common practice and all traders engage in personalised pricing.

(71) Overall, the new information obligation of the Consumer Rights Directive, as amended, is at best a conspicuously incomplete short-term solution but fails to tackle the problem of the digital asymmetry between traders and consumers.

d) Unfair commercial practices beyond the scope of the Consumer Rights Directive?

(72) As mentioned above, a breach of the information obligation under the Consumer Rights Directive automatically constitutes an unfair commercial practice under Article 7(5) UCPD but only as much as the new information obligation of the Omnibus Directive, Article 7(5) UCPD operates at the surface level. In the following section, we discuss whether other grounds of unfairness appear in the terms of the UCPD.

e) Misleading omission

(73) Beyond the scope of the Consumer Rights Directive, no explicit information obligation has been adopted in EU consumer law. Still, nontransparent personalised prices could be a misleading omission under the terms of Article 7(1) Unfair Commercial Practices Directive 2005/29/EC. To that end, information on personalised pricing has to be 'material'. Whether or not information is material depends on the consumer's knowledge and expectations; these in turn are formed by the consumer's socio-cultural background.[106]

(74) Here, the traditional equal price policy of traders is relevant.[107] Consumers are used to being charged equal prices, and they react with disaffirmation when confronted with personalised pricing.[108] This will even be affirmed by the new information obligation of the Consumer Rights Directive, as consumers will certainly not assume that some traders have to lay open personalised pricing strategies whereas others do not.

(75) That the issue of being subjected to such strategies or otherwise will be relevant for their decision to interact with the trader in question has just been confirmed by the decision of the EU legislator to introduce Article 6(1)(ea) Consumer Rights Directive. The limited scope

---

105 P. Rott and O. Lynskey, A Universal Regulatory Framework for Powerful Online Platforms (BEUC, 2020).

106 See also T. Wilhelmsson, Misleading practices, in G. Howells, H.-W. Micklitz and T. Wilhelmsson (eds), *European Fair Trading Law* (Aldeshot, Ashgate, 2006), 123, 152.

107 This strategy had been pursued since the mid-19th century, see Zander-Hayat, Reisch and Steffen, n. 66, 403.

108 See P. Rott, A Consumer Perspective on Algorithms, in L. de Almeida, M. Cantero Gamito, M. Durovic and K.P. Purnhagen (eds), *The Transformation of Economic Law* (Hart Publishing, 2019), 43, 47; W. van Boom, J.-P.I. van der Rest, K. van den Bos and M. Dechesne, Consumers Beware: Online Personalised Pricing in Action! How the Framing of Mandated Discriminatory Pricing Disclosure Influences Intention to Purchase, *Social Justice Research* 33 (2020), 331, 332, both with further references.

of that decision cannot possibly be interpreted so that there should be different treatment between commercial communication within and without the scope of application of that Directive. Rather, it must be explained by the fact that general consumer law was under review, with the fitness check of consumer and marketing law, while other areas of consumer law were not, and perhaps by the fact that the information obligation was included hastily quite late in the legislative process.

(76) Information about personalised pricing strategies is therefore material information under the terms of Article 7(1) Unfair Commercial Practices Directive, and it causes or is likely to cause the average consumer to take a transactional decision that they would not have taken otherwise. Therefore, even outside the scope of application of the Consumer Rights Directive, traders have to inform consumers about their use of personalised pricing strategies.[109] That position has, however, not yet been confirmed by the Court of Justice.

f) Unfairness for other reasons?

(77) As explained more generally in the Area 1 study, even where the fact that prices are personalised are laid open, that fact alone does not remedy the digital asymmetry between traders and consumers, as the consumer has no possibility to understand how the price was personalised, or whether they benefit from or are disadvantaged by personalisation when compared to the 'average' consumer (of which group?). Moreover, personalisation may be based on personal data the consumer has shared voluntarily, or on data retrieved unlawfully by that particular trader, or acquired from other traders that may have collected data unlawfully or were not allowed, under the limited consent given by the consumer, to pass them on. And, as discussed below, even seemingly voluntary consent may have been unduly influenced by the trader.[110]

(78) This link is at least not openly reflected in the current interaction between the GDPR and the UCPD. As mentioned above, it would seem highly impractical for a consumer to explore what personal data each trader that (openly) uses personalised prices has and where it got that information from. The only way to protect the consumer would be to consider personalisation on the basis of personal data acquired or passed on unlawfully as an unfair commercial practice. Indeed, one could argue that breaching the GDPR and also exploiting someone else's breach of the GDPR constitutes a violation of professional diligence and therefore an unfair commercial practice under the terms of Article 5(2) UCPD. Not least, the trader may gain a competitive advantage over other traders that comply with data protection laws. Moreover, given the general disapproval of price personalisation, and even more on the basis of unlawfully collected data, it would seem possible for the claimant to

---

109 See also Zander-Hayat, Reisch and Steffen, n. 66, 407 f.; E.I. Obergfell, n. 60, 298; Tillmann and Vogt, n. 64, 452 f.

110 See, e.g., Weinzierl, n. 46, 8 ff.

show that the practice materially distorts or is likely to materially distort economic behaviour of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers – whereby only the trader has information on the group of consumers it targets.

(79) The practical problem linked to this approach is that it is only with great difficulty pursuant to data protection law, if at all, that it is possible to find out whether or not that data was collected lawfully. Thus, the solution can only be found in relation to the preceding steps, namely, the requirements for collection of data and for data trading, as discussed below.

g) Competition law

(80) Beyond the interests of individual consumers, exploitation by way of personalised pricing could constitute abuse of a dominant position under the terms of Article 102 TFEU. According to the established case law of the Court of Justice, competition law serves, among other purposes, to protect consumers,[111] which includes individual consumer interests.[112] The European Commission has described the relevant consumer interests as comprising lower prices, better quality and a wider choice of new or improved goods and services.[113] More recently, however, the focus was also directed towards non-monetary interests. A prominent example is the *Facebook* decision of the German *Bundesgerichtshof* that turned on the (non-monetary) data protection interests of consumers.[114]

(81) Of course, one major limitation of a competition law approach to personalised pricing lies in the requirement of a dominant position in the market; which the *Bundesgerichtshof* easily found for Facebook in the social media market but which cannot possibly be assumed for all the retailers that potentially apply personalised pricing strategies. If that barrier can be overcome, the behaviour of that dominant player must be abusive; and in that value judgment, consumer interests can be integrated in the balancing of interests.

(82) The first step is of course to identify relevant consumer interests. Here, the European Commission favours a normative approach that relies on the average consumer whose interests are normative loaded by EU legislation.[115] In this sense, the new information

---

111 See ECJ, 6/10/2009, Case C-501/06 *GlaxoSmithKline Services Unlimited v Commission*, ECLI:EU:C:2009:610.

112 See ECJ, 13/7/2006, joined Cases C-295/04-C-298/04 *Vincenzo Manfredi v Lloyd Adriatico Assicurazioni SpA*, ECLI:EU:C:2006:461.

113 Communication from the Commission, Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, OJ 2009 C 45/7, para. 5.

114 BGH, 23/6/2020, KVR 69/19, *Gewerblicher Rechtsschutz und Urheberrecht* 2020, 1318; on which see R. Endler, Die Interessen der Verbraucher im Kartellrecht am Beispiel der Facebook-Entscheidung des BGH, *Verbraucher und Recht* 2021, 3 ff.

115 For example, in its *CECED* decision, the Commission, in its analysis of benefits to the consumer, referred to the collective environmental benefits of reduced energy consumption of washing machines, as supported by then Art. 174 TEC; see European Commission, Decision 2000/475/EC of 24/1/1999, Case IV.F.1/36.718.CECED.

obligation on personalisation of prices – with its underlying assumption that transparency in this regard is in the interest of the average consumer – can be considered, making fairness in price generation, or at least flagging up potential unfairness, a relevant consumer interest. In contrast, one can also investigate relevant consumer interests by empirical methods, as the *Bundesgerichtshof* did in its Facebook decision. Given the above-mentioned studies on consumer perceptions related to personalised prices, the result would be the same. In addition, the average consumer clearly has an interest in low, or fair, prices.[116]

(83) Consumer interest would then have to be balanced with the trader's legitimate interest in making a profit, or rather increasing its profit. In doing so, unlawful methods must be excluded; thus, secret personalisation at the expense of at least one part, and probably the bigger part, of consumers could constitute abuse of a dominant position. Where the dominant trader openly engages in personalised prices, the decision would depend on the validity of the criteria of price differentiation. Discriminatory criteria, such as religion, would make personalisation abusive. In terms of other criteria, the only remaining element of unfairness would seem to be nontransparency of prices. One decisive issue would then seem to be whether or not the consumer can avoid that particular trader or whether they are trapped – which latter situation the *Bundesgerichtshof* found in the case of Facebook. Surely, an individual retailer would find it difficult to produce lock-in effects that come anywhere near those that were decisive in the Facebook decision. The situation could, however, change if all competing traders engaged in personalised pricing, as consumers could no longer avoid personalisation at all.

(84) Overall, however, competition law would not seem to be the most effective area of law to challenge price personalisation, not least due to the fact that application of Article 102 TFEU requires a dominant position on the part of the trader. Outside and beyond Article 102 TFEU, a debate is proliferating between competition lawyers and supervisory authorities on whether personalised pricing is beneficial to competition or not. That debate falls outside the scope of this study.

4. Remaining options for the Member States?

(85) Given the very limited usefulness of EU law, individual Member States might consider introducing more stringent national law, such as a ban on personalised pricing. However, both the Consumer Rights Directive and the Unfair Commercial Practices Directive are total harmonisation directives (within their limited scopes of application), which triggers the question whether a Member State could still do that.

---

116 See also R. Endler, *Verbraucher im Kartellrecht*, 2020, 340, forthcoming.

a) The Consumer Rights Directive

(86) First of all, the mere fact that traders have to inform consumers if they personalise prices on the basis of automated decision-making does not necessarily mean that this could not be prohibited at the national level. To that end, one can refer to the consumer credit case of *Volksbank Romania* that turned on the compatibility with the Consumer Credit Directive 2008/48/EC of a national prohibition of certain bank charges. The Court held that whilst the Directive fully harmonised information obligations related to such charges, it did not regulate their admissibility at all. Thus, Member States still enjoy regulatory freedom in this area.[117]

(87) However, the Omnibus Directive 2019/2161/EU adds the above-mentioned recital (45), according to which '(t)raders may personalise the price of their offers for specific consumers or specific categories of consumer based on automated decision-making and profiling of consumer behaviour allowing traders to assess the consumer's purchasing power'. The term 'may' in this sentence is not, though, meant to be explicit permission to traders to use personalised pricing strategies but rather expresses the possibility that traders may do so. Thus, in the light of *Volksbank Romania*, a national prohibition of personalised pricing should not be considered as banned by the Consumer Rights Directive.

(88) Outside the scope of the Consumer Rights Directive, its total harmonisation approach does not take effect in any event.

b) The Unfair Commercial Practices Directive

(89) Whereas the Unfair Commercial Practices Directive generally pursues a total harmonisation approach, it has spared certain areas, and in particular financial services (see Article 3(9) UCPD). Thus, in these areas, Member States can declare commercial practices unfair that would not otherwise be regarded as unfair under the Directive.

(90) Where no exception applies, it seems difficult to argue that personalised pricing can be generally banned as a misleading practice where traders do so openly so that no misleading omission is involved, and it could not be generally be declared unfair where the data used for personalisation has been acquired lawfully. Moreover, personalised pricing could not be declared automatically unfair under national law, as according to the established case law of the Court of Justice, only commercial practices that form part of the black list can be considered unfair *per se*.

---

117 See ECJ, 12/7/2012, Case C-602/10 SC Volksbank România SA v Autoritatea Naţională pentru Protecţia Consumatorilor – Comisariatul Judeţean pentru Protecţia Consumatorilor Călăraşi (CJPC), ECLI:EU:C:2012:443.

5. Conclusion

(91) EU law appears to allow personalised pricing, subject to the data protection constraints discussed below, as long as it happens openly. The underlying problem of what data is used for personalisation, how that data is used and whether that data was obtained lawfully in the first place is at best, and only insufficiently, approached via data protection law, which is linked with neither contract law nor unfair commercial practices law. The situation somewhat recalls the long-standing separation of unfair commercial practices law and contract law, whereby an unfair commercial practice did not necessarily trigger consequences for the individual contract; a situation that will only be remedied (in many Member States) with implementation of the Omnibus Directive (EU) 2019/2161.

(92) Moreover, even the information obligation of the Omnibus Directive (EU) 2019/2161 can only be an interim solution to at least the transparency problem, as information will become obsolete once there is no more practical choice to avoid personalized prices.

III. Personalised commercial practices: The Current EU Legal Framework

(93) No explicit rules in the GDPR or in the UCPD deal with personalised commercial practices. The Omnibus Directive has not introduced any amendment that could be relevant for an assessment of personalised advertising. Therefore, the rationale is rather simple. Collection and processing of personal data for marketing purposes comes under the scope of the GDPR. As long as collection and further processing complies with the GDPR, the Regulation does not set any limits to personalised marketing techniques.

1. Data Protection law

(94) Under the GDPR, processing personal data is deemed lawful if it has a legal basis (under Article 6 GDPR) and complies with the data processing principles in Article 5 GDPR (fleshed out in later provisions). Compliance of personalisation practices with these two elements of the GDPR will therefore first be considered before turning to more specific rights of the individual data subject that are relevant in this context, in particular the prohibition of automated decision-making found in Article 22 GDPR and the right to information and an explanation derived from Articles 13-15 GDPR.

a) A Legal Basis for Personal Data Processing

(95) In order to be lawful, personal data processing must have a legal basis.[118] In its Guidelines, the European Data Protection Board (EDPB) indicates in the online behavioural advertising context that the Article 6(1)(b) legal basis – where processing is necessary to enter into or perform a contract – cannot be relied upon simply because advertising indirectly funds provision of the service. It notes that:

> Although such processing may support the delivery of a service, it is separate from the objective purpose of the contract between the user and the service provider, and therefore not necessary for the performance of the contract at issue.[119]

(96) In its Guide to the GDPR, the UK Information Commissioner's Office (ICO) uses the example of online targeted advertising to illustrate that advertising clauses are likely to be ancillary to the main purpose of the contract and would therefore not be deemed necessary.[120]

(97) If such processing cannot be justified on the basis that it is necessary for contractual purposes, attention then turns to a likely alternative legal basis: consent or legitimate interests. The applicability of each will be considered in turn.

(98) Where personalisation is based on profiling facilitated by the use of a cookie or other online tracking technology (such as device fingerprinting) placed on the terminal equipment of a user, this initial data extraction must be based on consent pursuant to Article 5(3) E-Privacy Directive.[121]

(99) That consent must comply with the requirements of the GDPR. It must be specific, informed, unambiguous and freely given by the data subject.[122] These criteria are all relevant to personalisation practices.

(100) Specific consent requires that the activity or service accessed by the user is clearly separated from the act of giving consent. A user could not therefore give consent to profiling or personalisation by simply continuing to use a service following a pop-up box announcing such profiling. In *Planet49*, the Court of Justice held that consent lacked specificity as by clicking once on a participation button the user simultaneously participated in a lottery and

---

118 Art. 6 GDPR.

119 European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, adopted on 8 October 2019, 15.

120 ICO, *Guide to the GDPR*, available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf, 65.

121 For details, see D. Clifford, EU Data Protection Law and Targeting Advertising, n 43, 194

122 Art. 4(11) GDPR.

consented to installation of cookies.[123] Similarly, the French Data Protection Authority (DPA) Commission Nationale de l'Informatique et des Libertés (CNIL) held that that Google's advertising personalisation practices breached the GDPR and were not based on specific consent. The CNIL noted that before creating an account, a user was asked to tick a box agreeing to Google's Terms of Service and agreeing to personal data processing 'as described above and further explained in the Privacy Policy'. This blanket consent for all the processing operation purposes carried out by Google (speech recognition, ad personalisation and so on) was deemed incompatible with the principle of specificity.[124]

(101) Informed consent means that the user must be fully informed of the data processing conditions and there 'must be no room for ambiguity whatsoever'. The CNIL held that Google's ad personalisation practices also breached this criterion. The fact that Google's information on ad personalisation was spread over a number of documents did not enable the user to be fully aware of the extent of personalisation. It noted, for instance, that the section entitled 'Ads Personalization' did not fully inform the user of the 'plurality of services, websites and applications involved in these processing operations (Google search, You tube, Google home, Google maps, Playstore, Google pictures …) and therefore of the amount of data processed and combined'.[125] As the UK's Competition and Market Authority notes in its recent report on digital platforms, there is a concern that platforms' wider choice architecture encourages consumers to agree to use of their data for personalised advertising, by effectively inhibiting informed choice – through poor accessibility and clarity, unbalanced presentation and barriers to consumer action.[126]

(102) Unambiguous consent requires clear affirmative action on the part of the data subject. In *Planet49*, the Court considered that pre-ticked consent boxes could not be considered unambiguous. It held that requiring a user to positively untick a box and therefore become active if they do *not* consent to installation of cookies does not satisfy the criterion of active consent. Similarly, the CNIL noted that Google relied on pre-ticked boxes when obtaining consent for ad personalisation and that this was not sufficiently 'unambiguous' to be GDPR-compliant.

(103) Perhaps the most contentious aspect of consent is when it can be said to be freely given and, in this context, whether providing consent when significant digital asymmetry is at play vitiates that consent. Consent cannot be freely given in situations of imbalances of power,

---

123 For a summary of the findings see: CNIL, *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*, 21 January 2019. Available at https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

124 Ibid.

125 Ibid.

126 Competition and Markets Authority, *Online platforms and digital advertising*, Market study final report, 1 July 2020 ('the CMA Report'), 194.

as the Court of Justice confirmed in *Schwarz.*[127] This case concerned the coercive power of the State. However, the EDPB indicated that, in its view, such imbalances of power are not confined to public authorities and employers. Rather, it suggests that:

> consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will.[128]

(104) Article 7(4) GDPR elaborates on when consent can be freely given. In making this assessment, 'utmost account' needs to be taken of whether 'the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.' This could be interpreted as a qualified prohibition on bundling data processing operations. This is particularly relevant in situations, prevalent online, where a service is provided for free at the point of access but subsidised through provision of targeted advertising. In such circumstances, should personal data processing be deemed *necessary* for provision of the service?

(105) In his Opinion in *Planet49*, the Advocate General opined on the offer in that case. In exchange for free-of-charge participation in an online lottery, users were required to consent to the processing of their personal data and commercial contact by up to a maximum of 30 companies (found in a list of 57 companies). This commercial contact could be by post, telephone, e-mail or SMS. In assessing whether such consent could be said to be freely given, and in particular whether it should be deemed *necessary* for performance of the contract, the Advocate General opined that it was. He observed as follows:

> it should be kept in mind that the underlying purpose in the participation in the lottery is the 'selling' of personal data (i.e. agreeing to be contacted by so-called 'sponsors' for promotional offers). In other words, it is the providing of personal data which constitutes the main obligation of the user in order to participate in the lottery. In such a situation it appears to me that the processing of this personal data *is* necessary for the participation in the lottery.[129]

(106) This issue was not addressed by the Court in its judgment. However, the question it raises is whether the data processing undertaken bears a reasonable relation to the service offered to the individual without monetary cost.[130] This is a much broader view of 'necessity for the performance of the contract' than that stated by the EDPB (above), for instance. Moreover, in its Guidelines on Consent the EDPB has stated that the GDPR 'ensures that the processing

---

127 ECJ, 17/10/2013, Case C-291/12, *Michael Schwarz v Stadt Bochum,* ECLI:EU:C:2013:670, para. 32.

128 Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.0, adopted on 4 May 2020, 8.

129 Opinion of AG Szpunar, 21/3/2019, Case C-673/17 *Planet49 GmbH*, EU:C:2019:246, para. 99.

130 O. Lynskey, General Report Topic 2: The New EU Data Protection Regime, in J. Rijpma (ed.), *The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection* (Eleven International Publishing, 2020) 23, 42 f.

of personal data for which consent is sought cannot directly or indirectly become the counter-performance of a contract'.[131]

(107) Looking at existing national practice on this issue, no consensus has yet emerged. The Italian Supreme Court has held that a website providing services can legitimately condition provision of the service on processing of data for advertising purposes, provided that consent is individually given and linked to the specific purpose, thus implicitly accepting that advertising was necessary for performance of the contract. The Austrian Supreme Court has examined this issue in the context of a collective action against a TV service provider regarding clauses in its general terms and conditions. It concluded that if conclusion of the contract is made conditional on consent to processing of personal data that is independent of the contract, it cannot be assumed that consent is freely given. The Supreme Court considered that such a strict interpretation of when consent is freely given can be derived from Articles 4(11), 7(4) and recital (43). What seems to distinguish the two cases is that, in the former, data processing subsidises the services whereas in the latter data processing was in addition to a fee charged to consumers.

(108) In interpreting the conditionality requirement (that performance of the contract is conditional on consent), one factor that may be relevant is whether alternatives are available to the data subject. The Austrian DPA considers that withholding a service in the absence of consent is lawful if the individuals affected had a choice and could receive the same service through a paid option which did not entail personal data processing. In that case, an online newspaper presented affected individuals with the option of either purchasing a paid subscription for €6 monthly or accessing the content free of charge but granting consent to the use of cookies for advertising purposes. The DPA concluded that such consent could be given freely, since the absence of consent would not cause any major disadvantage. In particular, it considered that, amongst other things, the online subscription was not excessively expensive; other newspapers provided news and the content could be accessed in print form.

(109) The lessons that can be drawn from this mixed picture of personalised marketing are unclear. On the one hand, there is a recognition that digital content and services made available without monetary cost need to be funded and that commercial data processing fulfils this function. On the other hand, the necessity criterion invites us to consider whether the personal data processed is excessive in relation to the content or service offered without monetary cost. In measuring this cost, we are reminded of the test for excessive pricing in competition law, which queries whether a dominant firm's pricing strategy allows for a reasonable (rather than excessive) return on investment. Data protection authorities have not yet approached the test in this way, although the Austrian DPA did note that alternative

131 Guidelines 05/2020, n. 128, 10.

options were not 'excessively expensive'. This is perhaps because of a reluctance to act as proxy price regulators. Nevertheless, this aspect of the GDPR as well as others (such as data minimisation) requires them to make such assessments.

(110) Indeed, one of the most far-reaching interventions in this context has come from a competition and consumer authority, the CMA, which recommends that the UK government introduces legislation to provide a Digital Markets Unit with new relevant powers. In particular, it recommends a 'choice requirement', whereby digital platforms would be required to provide consumers with the choice not to share their data for the purposes of personalised advertising.[132] The regulator would also have the power to influence presentation of choices including defaults. This, it suggests, would 'rebalance the relationship between platforms and their users', thereby alleviating the digital asymmetry. Where a user decides not to share their personal data, they should still be able to access the basic or core service of the platform and they would continue to see non-personalised advertising. This is a recommendation that we would endorse.

(111) Beyond consent, discussion is ongoing about whether the legitimate interests of the controller or third parties might provide a suitable legal basis for processing for personalisation purposes. Recital (47) GDPR leaves this possibility open as it states that:

> The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

(112) In its Opinion on Purpose Limitation, the Article 29 Working Party indicated that this is in principle not possible. It stated that:

> when an organisation specifically wants to analyse or predict the personal preferences, behaviour and attitudes of individual customers, which will subsequently inform 'measures or decisions' that are taken with regard to those customers .... free, specific, informed and unambiguous 'opt-in' consent would almost always be required, otherwise further use cannot be considered compatible.[133]

(113) This Opinion was issued prior to adoption of the GDPR. Nevertheless, it remains unlikely that the opinion of data protection authorities, at least, on this matter will have changed. For instance, in 2019 the UK's DPA, the Information Commissioner's Office, considered that in the context of personalised digital advertising, it is unlikely that legitimate interests could

---

132 CMA Report, n. 126, 379.

133 Art. 29 Working Party, *Opinion 3/2013 on purpose limitation*, adopted on 03.04.2013 (WP203) section III.2.5 and Annex 2.

justify the intensive data processing involved.[134] One might further argue that the principle of fairness must be taken into consideration when applying the legitimate interests test.[135]

b) Fairness

(114) As Zuiderveen Borgesius notes, in situations where anti-discrimination law is difficult to apply to algorithmic decisions (for example, where there are inaccurate predictions that are difficult to correlate to the protected categories in anti-discrimination law), the principle of fairness found in the GDPR may be of use. In other words, some actions can be unfair even if not discriminatory.[136] Although some consider fairness to be the overarching rationale for the right to data protection found in Article 8 EU Charter,[137] its precise meaning and application in situations of digital asymmetry remains to be fleshed out.[138] Nevertheless, ample evidence is available of application of the principle at national level in EU Member States. For instance, in Slovenia violations of the principle of fairness have been the most frequently investigated in recent years.[139]

(115) The predominant understanding of fairness connects it to the transparency principle. Article 5(1)(a) GDPR provides that personal data shall be processed 'lawfully, fairly and in a transparent manner'. The EDPB has, for instance, indicated that the provision of appropriate information in relation to automated decision-making is particularly relevant in respect of the fairness of data processing. At national level, a Belgian court has held that lack of sufficient information about Facebook's systematic tracking of internet users on third party websites (irrespective of whether they were Facebook users) violated the principle of fair processing.[140] Malgieri considers that a distinction exists between transparency and fair transparency. He suggests that beyond the formalistic information requirements, fairness requires a more considered approach that mandates additional analysis of the circumstances and context in which data processing takes place.[141]

---

134 ICO, *Update Report into Adtech and Real-time Bidding*, 20 June 2019, 18. Available at: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.

135 I. Graef, D. Clifford and P. Valcke, Fairness and enforcement: bridging competition, data protection, and consumer law, 8(3) *International Data Privacy Law* (2018), 200, 203 f.

136 F.J. Zuiderveen Borgesius, Strengthening legal protection against discrimination by algorithms and artificial intelligence, *The International Journal of Human Rights* (2020), 13.

137 See H. Hijmans, The European Union as Guardian of Internet Privacy (2016, Springer).

138 Resort to the concept of fairness in other areas of law has been controversial. See, e.g., A. Jones, B. Sufrin and N. Dunne, *EU Competition law: Text, Cases and Materials*, 5th ed. (OUP, 2019), 31.

139 Lynskey, n. 130, 36.

140 ibid., 41 and, for further detail, 138 f.

141 G. Malgieri, The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation, in: *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (2020), 154.

(116) The principle has also been linked to good faith in some jurisdictions. For instance, in Austria the principle of fairness was violated when a controller operated a policy which entailed deletion of all personal data, even in situations where the data subject requested partial deletion.

(117) Perhaps of most relevance in this context is the application of fairness where a data processing practice contravenes the reasonable expectations of the data subject and where a violation occurs of another area of law.

(118) In the UK, fairness has been linked to the reasonable expectation of the data subject with regard to the processing of their personal data. The ICO has stated in its guidance that:

> In general, fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them.

(119) An ICO decision indicates how this might be applied in practice. It investigated data processing by a pregnancy and parenting club, which collected personal information for the purpose of membership registration through its website and mobile app, merchandise pack claim cards and directly from new mothers at hospital bedsides. The company also operated as a data broker service, supplying data to almost 40 third parties including credit reference and marketing agencies. The ICO decision concluded that the controller failed to use the personal data of the 14 million affected data subjects fairly. In particular, it found that data subjects 'registering with a pregnancy and parenting club would not reasonably have expected their personal data to be disclosed to the likes of credit reference, marketing and profiling agencies'.[142]

(120) Another important dimension of fairness in the context of personalisation is its relationship with the principle of legality in data protection law. According to Article 6(1) GDPR, processing is lawful only if and to the extent that one of the legal bases applies. However, the principle of 'lawfulness' in Article 5(1)(a) is arguably broader and could be interpreted to mean that data processing must comply with other areas of law. Such a requirement could also be said to stem from the principle of purpose limitation, which requires the purposes of personal data processing to be 'legitimate'.[143]

(121) Such an interpretation requires the GDPR to use other areas of law as a normative benchmark for its application.[144] This approach finds some support in national decisional practice. For instance, the Hungarian Constitutional Court has held that personal data may

---

142 ICO, *Monetary Penalty Notice to Bounty (UK) Ltd*, 11, available at https://ico.org.uk/media/action-weve-taken/mpns/2614757/bounty-mpn-20190412.pdf.

143 Art. 5(1)(b) GDPR.

144 The converse has also been argued; that another branch of law should use the GDPR as its normative benchmark. See F. Costa-Cabral and O. Lynskey, Family ties: the intersection between data protection and competition in EU Law, *Common Market Law Review* 54 (2017), 11.

only be processed for a legally-justified purpose and that every stage of processing must conform to this, linking this interpretation to fairness.[145] The UK's Information Commissioner has suggested that if contact tracing applications were used to discriminatory effect (to exclude individuals with disabilities from employment or social opportunities, for example), then data protection principles such as fairness, proportionality and transparency are critical.[146]

(122) Such a consistent approach between interconnected areas of law – sectional coherence – is helpful in tackling digital asymmetries.[147] As Majcher observes, whether such a consistent approach is mandated by the EU Treaties is debatable. Article 7 TFEU states:

> The Union shall ensure consistency between its policies and activities, taking all of its objectives into account and in accordance with the principle of conferral of powers.

(123) Consumer protection and data protection both sit amongst the 'provisions of general application' in the TFEU and enhance the EU's overarching objectives to ensure the well-being of its peoples and to develop a competitive social market economy.[148] At a minimum, therefore, Article 7 should ensure that related laws and policies are interpreted in a way that is not contradictory. However, as Majcher observes, this principle could also be read as a 'broader and more demanding principle implying the presence of positive connections between different elements of the legal system in pursuing certain objectives'.[149] Such a consistent interpretation between data protection and neighbouring branches of law is confirmed by the text of the GDPR, strengthening the claim for such an interpretation of Article 7 TFEU. Data protection law could therefore reach out to anti-discrimination law to consider what is unfair, as the Finnish DPA did when finding that the way a credit information company was establishing credit scores was discriminatory as a very low or high age would cause an application for credit to be automatically inadmissible.[150] It could also reach out to consumer protection law to interpret the notion of 'fairness', particularly given common concepts such as deception. The ICO, for instance, has held that whether or not personal data is processed 'fairly' depends on how it was obtained, in particular whether or not the data subject was 'deceived or misled when it was obtained'.[151]

---

145 Lynskey, n. 130, 36.

146 Houses of Parliament, Joint Committee on Human Rights, Oral evidence (virtual proceeding): The Government's response to Covid-19: human rights implications, HC 265, 4/5/2020, Q25.

147 Majcher defines this type of coherence as coherence between legal rules that belong to two or more different areas or branches of the same legal system. K. Majcher, *Coherence between EU Data Protection and Competition Law in the Digital Market* (PhD Thesis, VUB), submitted on 27/5/2020, 15.

148 Art. 3(1) and 3(3) TEU respectively.

149 Majcher, n 147, 169.

150 Lynskey, n. 130, 36.

151 ICO, n 120, 22.

c) The Prohibition on Automated Decision-Making

(124) Once within the material scope of application of the legal framework, much of the focus has been on Article 22 GDPR in the context of automated decision-making. This provision provides that:

> The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.[152]

(125) While the provision sits alongside the rights granted to data subjects in the GDPR, according to the EDPB, Article 22 should be read as a prohibition rather than a right that must be invoked by data subjects.[153] Such an interpretation is necessary, as Kaminski suggests, as interpreting Article 22 GDPR as a right would, counterintuitively, limit the protection it offered by allowing data controllers to 'regularly use algorithms in significant decision-making, adjusting their behaviour only if individuals actually invoke their rights'.[154]

(126) Nevertheless, as a prohibition it is subject to a number of significant caveats, which have led to scepticism regarding its utility in addressing algorithmic personalisation.

(127) First, the prohibition itself applies to profiling based *solely* on automated decision-making. This also excludes situations where a suggestion based on automated decision-making is rubber-stamped by a human without any meaningful oversight.[155] Given that such human oversight of personalised pricing and marketing techniques is highly unlikely, this qualification is of little relevance in this context.

(128) Second, the requirement that an automated decision must produce legal effects or 'similarly significantly affect' the data subject could be an important impediment to the application of this prohibition to personalisation practices. A legal effect is one that affects an individual's legal rights or status, including under a contract, such as cancellation of a contract.[156] What constitutes a 'similarly significant' effect to a legal one is more uncertain. Such effects must be 'sufficiently great or important to be worthy of attention' by having the potential to:

- significantly affect the circumstances, behaviour or choices of the individuals concerned;
- have a prolonged or permanent impact on the data subject; or

---

152 Art. 22(1) GDPR.

153 EDPB, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, (WP251rev.0), adopted on 6 February 2018 (EDPB, ADM Guidelines)

154 M. Kaminski, The Right to Explanation, Explained,)34 *Berkeley Technology Law Journal* (2019), 190, 196.

155 I. Mendoza and L. Bygrave, The Right not to be Subject to Automated Decisions Based on Profiling, in T.E. Synodinou et al. (eds), *EU Internet Law: Regulation and Enforcement* (Springer, 2017) 77, 87; EDPB, ADM Guidelines, n. 153, 21.

156 EDPB, ADM Guidelines, n. 153, 21.

- at its most extreme, lead to the exclusion or discrimination of individuals.[157]

(129) Recital (71) provides some examples, including credit determinations and e-recruitment practices conducted solely by automated means. The EDPB adds to these examples, suggesting that decision-making that affects someone's financial circumstances, access to health or education or disadvantages their employment prospects has such an effect.[158] Specifically, with regard to personalised pricing practices, the EDPB suggests that they could meet this threshold if, for instance, 'prohibitively high prices effectively bar someone from certain goods or services'.[159]

(130) The EDPB Opinion considers that the standardised practice of profiling and personalised marketing would not meet this threshold. However, it opines that the particular nature of the personalisation practice would need to be taken into consideration. It suggests that the following characteristics could be taken into consideration:

- the intrusiveness of the profiling process, including tracking individuals across different websites, devices and services;
- the expectations and wishes of the individuals concerned;
- the way the advert is delivered; or
- using knowledge of the vulnerabilities of the data subjects targeted.[160]

(131) Given the extent to which profiling for personalisation purposes draws on data extracted from cross-platform browsing activity and defies the expectations of data subjects, it is arguable that this brings even 'mainstream' personalisation practices within the scope of Article 22 GDPR.

(132) Third, the prohibition does not apply where the data subject explicitly consents,[161] where processing is necessary to enter into or perform a contract,[162] or where authorised by Union or Member State law.[163] In such circumstances, automated personalisation can occur even if impacting on individuals. However, where Member State law allows for this possibility, it must lay down 'suitable measures to safeguard the data subject's rights and freedoms and legitimate interests'.[164] Similar requirements exist where decision-making is based on consent or contract but stipulates that this should include 'at least the right to obtain human

---

157 Ibid.

158 Ibid, 22.

159 Ibid, 22.

160 Ibid.

161 Art. 22(2)(c) GDPR.

162 Art. 22(2)(a) GDPR.

163 Art. 22(2(b) GDPR.

164 Art. 22(b) GDPR.

intervention on the part of the controller, to express his or her point of view and to contest the decision'.[165]

(133) A generous interpretation of personalisation practices that significantly affect an individual could therefore lead to the prohibition of such practices or, at a minimum, the availability of 'due process' safeguards for individuals such as the right to contest the decision and obtain human intervention.[166] Moreover, the Guidelines suggest that this also entails systemic accountability measures such as algorithmic auditing and ethical review boards.[167] Therefore, while the GDPR does not contain a prohibition on personalisation practices, it does constrain their operation in a meaningful way. For some, its principal drawbacks will be that it requires a contextual assessment of personalisation practices (as opposed to a more categorical approach) which can be difficult to assess the legality of given the opacity of algorithmic decision-making.

d) Transparency and the Right to Explanation

(134) Accompanying the Article 22 GDPR prohibition are complementary measures which seek to shed more light on opaque algorithmic decision-making practices. While the Parliament had inserted an additional safeguard into the text of (then) Article 20 on profiling, the right to obtain an explanation of the decision reached after such an assessment, this 'right' was subsequently relegated to recital (71).[168] Several of the information requirements in the GDPR also relate to automated decision-making. At the point where personal data are obtained or within a reasonable period thereafter, and with the aim of ensuring fairness and transparency, the controller is obliged to provide the data subject with information regarding the 'existence of automated decision-making, including profiling' and 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'.[169] Furthermore, once personal data processing is under way, the data subject also has access to such information pursuant to their right of access in Article 15(1)(h).

(135) There has been much heated doctrinal debate as to whether a 'right to explanation' of algorithmic decision-making, including personalisation practices, can be deduced from the

---

165 Art. 22(3) GDPR.

166 D. Keats Citron and F. Pasquale, The Scored Society: Due Process for Automated Predictions, 89(1) *Washington Law Review* (2014), 1 ff.

167 EDPB, ADM Guidelines, n. 153, 32; M. Kaminski, Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability, 92 *Southern California Law Review* (2019), 1529.

168 Position of the European Parliament adopted at first reading on 12 March 2014 with a view to the adoption of Regulation (EU) No .../2014 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), EP-PE_TC1-COD(2012)0011, Article 20(5).

169 Arts 13(2)(f) and 14(2)(g) GDPR.

GDPR. Wachter et al define such a right narrowly as a right to *ex post* explanations of specific decisions addressing the data subject, and suggest that the GDPR contains no such right.[170] They argue in favour of a right to be informed of the system functionality of automated decision-making. These claims are justified on two key grounds. First, that the reference to a right to explanation which would contain a right to *ex post* specific explanations was removed from the safeguards in Article 22(3). Second, that the requirement of 'meaningful information' found in Articles 13-15 has an identical meaning across these provisions. As Articles 13-14 require provision of such information prior to automated decision-making and they surmise specific explanations cannot be provided at that point, they suggest that such meaningful information is necessarily limited to *ex post* general system functionality information.

(136) On the other hand, this reading of the GDPR and the 'right to explanation' has been vigorously contested. Selbst and Powles suggest that the distinctions drawn between explanations pertaining to system functionality and specific decisions and the timing of explanations are artificial and premised on a misunderstanding of the technology. They acknowledge that neither an explanation of system functionality nor specific decisions will be possible in some machine learning contexts.[171] However, they suggest that, in the majority of instances, machine learning is deterministic – meaning that given the same inputs to the same model, the same outputs will result.[172] The consequence of this is that a complete system level explanation will also explain specific cases, and the system functionality/specific decision and *ex ante/ex post* distinction collapses.[173] More generally, scholars have emphasised that these provisions need to be interpreted purposively and that 'meaningful information' must be meaningful to the data subject in relation to the GDPR's aim of strengthening individual rights.[174] In France, for instance, public authorities relying on automated decision-making must reveal the 'principal characteristics' of the system to data subjects.[175] This includes information such as the extent to which automated processing contributed to a decision; the data processed and its source; parameters used and their

---

170 S. Wachter, B. Mittelstadt and L. Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law* 2017, 76.

171 A.D. Selbst and J. Powles, Meaningful information and the right to explanation, *International Data Privacy Law* 2017, 233, fn 39.

172 Ibid, 239.

173 Ibid, 239 f.

174 G. Malgieri and G. Comandé, Why a Right to Legibility of Automated Decision-making Exists in the General Data Protection Regulation, *International Data Privacy Law* 2017, 243; Selbst and Powles, n. 171, 236; Mendoza and Bygrave, n. 157, 93.

175 Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. Available at: https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000031589829/.

weighting; and 'operations' performed based on the processing.[176] Such criteria could also be relevant in determining what constitutes meaningful information for the data subject.

(137) It is possible to envisage other types of information that may be useful for the data subject to receive.[177] Nevertheless, these information-forcing obligations are significant, especially when combined with the more systemic powers available to data protection authorities to exercise oversight of automated decision-making. As Kaminski suggests, 'it is myopic to focus only on the individual version of transparency and decry its shallowness, rather than seeing its place and purpose in a system of required information flows'.[178]

(138) Nevertheless, a number of improvements might be suggested. The mechanisms foreseen in the GDPR relate primarily to past data processing practices. Where the training data and algorithm deployed are constantly changing, it is difficult to predict real time outcomes (as is the case with Google's search engine for instance). Marsden and Nicholls suggest that in such circumstances the only remedy is replicability 'taking an 'old' algorithm and its data at a previous point in time to demonstrate whether the algorithm and data became discriminatory'. They suggest that such a remedy is incomplete as it essentially uses a 'slow motion replay' as the game rushes on. One potential supplementary option available under the GDPR would be the use of processing suspensions while a complaint is under investigation. This is listed as a corrective power and so a *prima facie* finding of infringement may be a prerequisite for such a ban.[179]

e) Interim observations

(139) The role of data protection law in addressing personalisation practices should not be overstated. Personalisation practices, in particular personalised marketing, have societal implications that must be emphasised and expose some limits of data protection law. Protection of the individual in the GDPR, reflected in the definition of personal data and the rights granted to individuals, can lead to mismatches in the digital environment. As Tisné observes, personalisation can lead to inferred harms, where an individual is inferred as being part of a group based on the processing of third-party data. He gives the example of dating websites that try to ascertain sex-appeal based on facial characteristics; the harm of this activity may not impact those who upload their own photos. Optimisation also leads to externalities that the GDPR finds difficult to address, for instance when personalisation

---

176 Décret n° 2017-330 du 14 mars 2017 relatif aux droits des personnes faisant l'objet de décisions individuelles prises sur le fondement d'un traitement algorithmique. Available at: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000034194929/2020-10-06/.

177 L. Edwards and M. Veale, Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, 16 *Duke Law & Technology Review* (2017), 18, 77-80.

178 Kaminski, n. 154, 216.

179 Art. 58(2)(f) GDPR.

directs individuals to content that vilifies minorities. Such harms, stemming from 'a process of continuous observation and calibration of human behaviour rather than discrete instances of ad placement' point to the need for broader consideration of issues of automation and power (such as that considered in Area 3).

(140) Nevertheless nor, despite these limitations, should the potential role of GDPR in addressing digital asymmetry in the context of personalisation be downplayed. Taking the example of inferred harm mentioned above, even if a facial recognition algorithm was trained using the data of other third parties at the point where a 'decision' is made about the sex-appeal of an individual, then this falls within the GDPR and the targeted individual benefits from the rights and safeguards set out above. Similarly, invocation of general principles such as fairness and purpose limitation can address individual wrongs but also more widespread data processing practices. An initial, obvious, recommendation is to strive for a maximalist interpretation of these rights and safeguards in the digital environment and to move beyond their ostensible 'individualistic' focus, as advocated by Ausloos and Mahieu.[180]

2. *The effects of digital asymmetry through personalisation*

(141) The only further tools to exercise at least some sort of control over personalised commercial practices are to be found in Directive 2005/29/EC on commercial practices. In Area 1 we have analysed and explained universal and structural digital vulnerability, which justifies the assumption of digital asymmetry that requires a reversal of the burden of proof/burden of argumentation. The personalisation techniques that the marketing business has developed and is constantly refining lays bare that the consumer has no chance and no means to check the whole machinery which stands behind a single personalised commercial practice. At the very best the consumer has given their consent to collection of their personal data, but nobody can overlook how and by whom these data are used and exploited for money making purposes. The major sources of personalised data are cookies and social media. The most precious data are in the hands of the GAFAs and a handful of big companies which have the necessary resources and capacities to collect the data of their users, to process those data and to use them for marketing purposes.[181] It is near-impossible to find hard facts on data trading, let alone on the conditions under which data are traded.[182]

(142) In short, the consumer is confronted with personalised commercial practices without having the slightest idea why they are receiving the marketing and without having access to their

---

180 J. Ausloos and R. Mahieu, Harnessing the collective potential of GDPR access rights: towards an ecology of transparency, *Internet Policy Review.* 2020, available at https://policyreview.info/articles/news/harnessing-collective-potential-gdpr-access-rights-towards-ecology-transparency/1487.

181 This assessment is based on interviews H.-W. Micklitz led with McKinsey and marketing research institutions.

182 SVRV, Verbraucherrecht 2.0, n. 94.

alter ego on the internet: the profile that the supplier of the marketing has built itself or bought from somewhere. Taking asymmetry and the helplessness seriously, one might wonder whether and to what extent the cascade of UCPD remedies ranging from black listed practices down to professional diligence can be of much help.[183]

3. *Personalised commercial practices as aggressive commercial practices*

(143) In area 1 we laid down our understanding for interpreting the digital asymmetry enshrined in data privacy policies as a form of aggression which comes under the scope of the Directive. One might wonder whether personalised commercial practices are not even a stronger form of aggression than data privacy policies, for the simple reason that the consumer is personally addressed. It seems hard to conclude, though, that personalised commercial practices should be unlawful *per se* or whether and to what extent aggression needs to be concretised through 'additional measures'.[184]

(144) The German Cartel Office is inclined to understand Samsung's sales strategy as harassment, which appears in Article 8 UCPD as one possible form of aggression. The idea is rather simple: If you connect your Samsung TV to the Internet, you may first see banner ads for discount chains and streaming services across your screen.[185] One might qualify this strategy as a form of personalization – each and every consumer who buys a Samsung is confronted with the banner ads. The assessment of the German Cartel Office goes along with a growing resistance on the part of consumers to personalised commercial practices for the very same reason. Consumers feel harassed through the stubborn reiteration of personalised commercial practices which refer to a previous sale or a previous behaviour.

4. *Personalised commercial practices as misleading omissions*

(145) Personalised commercial practices transport specific information on an individual consumer through a combination of individual data and proxies. The more individual the marketing is, the more the consumer might be concerned because they feel addressed as an individual. However, a difference exists between standardised data exploitation strategies as analysed in Area 1 and the pre-designed quasi-individualised standardization marketing strategy under scrutiny in Area 2. However, the two Areas share in common the distinction between the ground level and the surface level. When it comes to discussing whether a trader is obliged *de lege lata* to disclose that it uses personalised commercial practices, both levels

183 Helberger, Micklitz, Sax and Strycharz, n. 2, chapter 3.

184 ibid.

185 https://www.spiegel.de/netzwelt/netzpolitik/samsung-bundeskartellamt-kritisiert-werbebanner-auf-fernsehern-a-8ca474e4-8040-4d03-85e3-11773d4084dd.

are affected. That is why it seems appropriate to test whether the UCPD requires the supplier to disclose what is termed personalised information.

(146) Article 7 UCPD does not contain an obligation to disclose information; it only prohibits misleading omissions. The language of the Directive looks rather promising as the trader is obliged to disclose 'material information' (on personalised pricing as material see above). What could be more material than information not only on the existence of personalised commercial practices on the surface level but on individual behavioural preferences and the profile of the alter ego, which reach deep into the ground level? In light of the rather restrictive approach the CJEU has taken so far, it seems highly unlikely that the Court would be ready to deduce from Article 7 an obligation on the part of the trader to disclose the degree to which marketing is personalised, let alone the type of personal information it has collected. Strategic litigation might nevertheless be helpful to demonstrate a potentially serious gap in Directive 2005/29/EC which can only be closed by the legislature.

(147) More particularly, the information referred to in Article 7 (4) UCPD essentially relates to the conditions of a potential contractual relationship which the consumer may enter into with a trader, as well as to the trader itself. The list does not fully correspond to the list of criteria for assessing an act of misconduct (Article 6 paragraph 1 UCPD). This does not seem to be a coincidence, because the obligation to disclose is an exception in the Unfair Commercial Practices Directive. The information catalogue does not contain any information on commercial communication as such. Consequently, information on the criteria which the trader has to meet in order to present a personalised advertisement do not fall under Article 7 (4) UCPD.

5. Personalised commercial practices and professional diligence

(148) If personalised commercial practices can neither be interpreted as a form of aggression nor as a form of misleading omission, they could still be regarded as an infringement of Article 5. One might wonder whether a trader who is using personalised advertising should be obliged to set up an audit enabling it not only to demonstrate that the technique does not infringe non-discrimination law or fundamental rights, but also to provide information on the personalization strategy applied, the parameters used and the origin of the data.[186]

186 For details, see Helberger, Micklitz, Sax and Strycharz, n. 2.

IV. Recommendations for Legislative Action

(149) On 28 September 2020, the European Parliament spelt out what MEPs expect from the revision of the rules governing the digital economy:[187]

> Online advertising, profiling, and personalised pricing: MEPs want the Commission to introduce additional rules on targeted advertising and micro-targeting based on the collection of personal data and to consider regulating micro- and behavioural targeted advertising more strictly in favour of less intrusive forms of advertising that do not require extensive tracking of user interaction with content.

(150) This statement confirms in rather soft political language what the current study demonstrates: the existing body of rules, whether the GDPR, the UCPD or the UCTD, are blunt weapons in gaining control over the dark side of personalised commercial practices. So far, the European Commission has not yet proposed measures that point in such a direction.

1. Overarching

- Mandate consistent interpretation of neighbouring legal frameworks. The level of consistency sought should move beyond preventing contradictory findings and outcomes and strive for cross-fertilisation and normative borrowing in these fields. This mandate needs to be accompanied by consideration of the procedural impediments to cooperation, as well as potential legal challenges such cooperation may entail.

2. Regulatory concepts

- Digital vulnerability and digital asymmetry could be anchored in the legislative framework of UCDP *de lege lata* i.e. in Article 5, 8 and 9.
- Reversal of the burden of proof/burden of argumentation for data exploitation strategies could be derived from the UCPD *de lege lata*.
- It would facilitate and accelerate adaptation of the UCPD to the digital economy and society if both rules were written down in a revised UCPD
- The UCPD should introduce a rule on non-manipulation by design complementary to Article 25 GDPR

187 https://www.europarl.europa.eu/news/en/press-room/20200925IPR87924/meps-spell-out-their-priorities-for-the-digital-services-act

3. *Blacklisted practices*

- Exploitation of personal situational vulnerabilities through personalised commercial practices should be prohibited
- Using psychographic profiles to exercise emotional and psychological pressure with the goal of selling products should be prohibited

4. *Personalised pricing*

- The trader should be obliged to inform the consumer, on request, of the individual preferences (the behavioural alter ego) on which the personalised price (commercial practice) is based.
- The trader must not base personalisation on criteria that breach anti-discrimination laws.
- For the purposes of personalisation, the trader must only use data that it has lawfully acquired. On request, the trader must prove the lawfulness of the data it uses to that end.

5. *Personalised commercial practices*

- The trader should be obliged to inform the consumer that a commercial practice is personalised
- The trader should be obliged to inform the consumer, on request, of the individual preferences (the behavioural alter ego) on which personalised commercial practice is based
- Endorse the CMA choice intervention requirement to address the bundling of access to content and services in exchange for personalisation. While such a choice requirement could be mandated under data protection law, this has not yet been done. Such a requirement could therefore be set out in an *ex ante* regulatory instrument (such as the one proposed in Area 3).
- Encourage DPAs to assess whether data processing practices for personalisation purposes bear a reasonable relationship to the service offered. While such an assessment has its challenges, a quantitative approach does not need to be taken.

Part III

A Universal Service Framework for Powerful Online Platforms

Orla Lynskey[1] and Peter Rott[2]

---

1 Associate Professor of Law at the LSE and Visiting Professor at the College of Europe, Bruges specialising in Digital Rights and Technology Regulation, in particular EU Data Protection Law.

2 Interim Chair of Civil Law, Commercial Law and Information Law at Carl von Ossietzky University of Oldenburg, Germany.

Part III: Table of Contents

I. Introduction

(1) In recent years, across the EU, policymakers and regulatory authorities at both national and supranational level have been grappling with the challenge of effectively regulating the actions of digital platforms. This has proven to be a difficult task for several reasons.

(2) First, the range of 'harms' and market failures that regulatory action seeks to address are diffuse. Some relate to the responsibility of digital platform services for the content that they host and promote on their platforms, for instance, whether digital platforms should be subject to an ongoing responsibility to remove illegal or harmful content. Other issues are ostensibly economic in nature, such as whether a digital platform should have the ability to 'self-preference' or promote its own goods or services above those of its competitors. The way in which digital platforms acquire and further process personal data raises further issues of both fundamental rights and fair competition. No one regulatory intervention is likely to tackle such diffuse challenges effectively. Rather, it is necessary to ensure that regulatory intervention is consistent across legal domains and is clear in its identification of the issues it seeks to remedy.

(3) Second, the term 'digital platform' is itself a wide one. It encompasses consumer communications platforms, search engines, e-commerce platforms, app stores and others. These platforms not only differ significantly in terms of the services that they offer, they are also very different in terms of their reach (both geographic and their user base).

(4) As a result of these challenges, regulatory focus has been honing in on 'platform power' and those actors on the market that occupy a position of systemic importance, whether from an economic or a societal perspective. The power of these platforms is multi-faceted: their content moderation capacity reflects a form of media power or power over opinion-formation; their ability to exclude rivals and downstream dependents or determine their conditions of access and operation reflects their economic or market power; and, their ability to sort and categorise society into groups and to determine their treatment on this basis confers a power that might be classified as informational, or even likened to state power.

(5) Not all digital platforms will have the capacity to exercise their powers in this way. If, for instance, a platform lacks economic or market power, it will not be able to exclude equally efficient rivals from the market. Or, if a platform has very few users, despite displaying and promoting misinformation it might not influence public opinion in a harmful way. As such, a 'one size fits all' regulatory approach to digital platforms may not be appropriate and asymmetric regulation, targeting those platforms with greatest economic and societal impact, may be preferable.

(6) From a consumer and citizen perspective, the economic and social dependence on digital platforms has been consistently increasing in recent years. The pandemic has accelerated this trend by shifting previously physical interactions, from meeting friends for a drink to medical appointments, into the digital sphere. Offline commercial transactions in brick-and-mortar shops have also become more difficult.

(7) The – perhaps only perceived – dependence of consumers (and others) on platforms makes consumers vulnerable to exclusion from their services by way of denial of access or suspension and termination of services, as well as to the conditions under which services are provided, and in particular to requirements on allowing platform service providers to use the consumers' personal data.

(8) Against this backdrop, this paper examines whether additional ex ante regulation is necessary or desirable in order to protect consumer sovereignty and fundamental rights in the context of digital asymmetries of power. In particular, it queries whether the case can be made for the categorisation of certain digital platforms as services of general interest ('SGI') and for the extension of related market and universal service obligations to these digital platforms on this basis.

(9) In this study, we first analyse the existing legal framework (II), consisting of competition law, general consumer law and fundamental rights law, demonstrating the limitations of the application of these legal frameworks to digital platforms and identifying a potential gap for ex ante regulation to fill. We then (III) set out the current legal framework for SGI (SGI) in the EU, as this may be a basis for future ex ante regulation of digital platforms. Finally, (IV) we examine whether the SGI regulatory model could be extended to digital platforms by querying (i) what methodology should be used to identify relevant platforms and (ii) what substantive obligations might be appropriate in this context. The final section of the report summarises some of the key findings (V).

II. The current legal framework

1. EU competition law

(10) EU Competition law provisions incorporate a prohibition on anti-competitive agreements (Article 101 TFEU), a prohibition on abuse of dominance (Article 102 TFEU) and a legislative framework designed to identify and prevent market concentrations that would 'significantly impede effective competition' (the EU Merger Regulation).[1] The first two provisions apply ex post, examining former or ongoing market conduct to

[1] Regulation (EC) No 139/2004 on the control of concentrations between undertakings OJ 2004, L 24/1.

see whether it hinders competition in a way that limits consumer welfare or harms market integration.[2] The EU Merger Regulation is an ex ante instrument that seeks to assess the impact of a transaction (a merger, acquisition or joint venture) on future competition.

(11) Given that a handful of digital operators own and control vast swathes of the platform environment, there has been much debate over whether the current competition rules are equipped to deal with the challenges brought about by increased digitization and the ensuing shifts in social and economic practices. In 2014, the European Data Protection Supervisor called for a more holistic approach to the application of data protection, competition and consumer protection rules precisely because of its assessment that the market dominance of certain digital platforms challenged the effective application of data protection rules and threatened broader rights such as dignity and autonomy.[3] There has subsequently been a flurry of recent reports on the impact of data (including personal data) on competition in digital environments and the role of digital platforms in the digital ecosystem. These include, most notably:

- Joint Report – *Autorité de la Concurrence* and *Bundeskartellamt*, 'Competition Law and Data', May 2016;
- EDPS Opinion 8/2016 'On the coherent enforcement of fundamental rights in the age of big data', September 2016;
- European Commission, Competition Policy in a Digital Era, April 2019 (the Special Advisors' Report);
- Unlocking Digital Competition: Report of the Digital Competition Expert Panel, March 2019 (the Furman Report - UK);
- Competition and Markets Authority, 'Online platforms and digital advertising Market study final report', July 2020.

(12) While these reports have subtly different focal points, what is evident from them and the surrounding doctrinal debates is that digitization leads to a number of market shifts that competition law principles must accommodate. The challenges documented in these reports range from consideration of whether existing theories of harm are capable of adapting to the digital environment to the redesign of merger control to reflect its specificities. It is beyond the scope of this paper to discuss these challenges in full; however attention is drawn to two issues that are of particular relevance to debates around the appropriate regulation of digital platforms. These concern (a) the

---

2 The goals of competition law are heavily contested. See, for instance, I. Lianos, 'Some Reflections on the Question of the Goals of EU Competition Law', *UCL - Centre for Law, Economics and Society, Research Paper* Series 3/2013.

3 EDPS Preliminary Opinion "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy", March 2014.

goals of competition law and the interpretation of the 'consumer welfare' standard and (b) market definition.

a) The goals of competition law and the assessment of when intervention is needed

(13) The goals of EU Competition law remain contested and have not been clarified by EU positive law.[4] Three of the most frequently referenced goals of EU competition law are economic freedom (preservation of the competitive structure of the market in line with ordoliberal thinking), market integration (ensuring that private enterprises do not erect artificial impediments to cross-border competition within the Internal Market) and the enhancement of consumer welfare (the promotion of lower prices, and more quality, choice and innovation on the market). Beyond these specific goals, competition policy is simply one tool in the EU legal framework to achieve the overarching aim of ensuring a 'highly competitive market economy' and 'an open economy with free competition'.[5]

(14) In the context of abuses of dominance and merger control, the Commission has focused its efforts primarily on examining the impact of a practice or transaction on consumer welfare. This focus stems from a concerted effort on the Commission's part to adopt a more economic-approach to the application of Competition law, as exemplified by the guidelines on exclusionary conduct under Article 102 TFEU.[6] This approach has received a mixed reception however from the CJEU.[7] The Court has, for instance, asserted in the context of an alleged anti-competitive agreement that there is nothing in the text of Article 101 TFEU to indicate that only those agreements that deprive consumers of certain advantages are illegal. Rather, it emphasized that the Treaty competition provisions aim 'to protect not only the interests of competitors or of consumers, but also the structure of the market and, in so doing, competition as such'.[8]

(15) Nevertheless, despite such resistance from the CJEU, consumer welfare remains the lodestar of DG Competition's decisional practice.[9] In principle, the consumer welfare standard is flexible enough to accommodate harms to non-price dimensions of competition. For instance, in *Microsoft/LinkedIn* the Commission departed from the

---

4 I. Lianos, 'Polycentric Competition Law', *Current Legal Problems* 2018, 161.

5 Protocol No. 27 on the Internal Market and Competition [2008] OJ C 115/09; Article 3(3) TFEU.

6 European Commission, 'Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings', OJ 2009, C 45/7.

7 S. Esayas, 'Data Privacy and Competition Law in the Age of Big Data', PhD, University of Oslo, October 2019, 25-28.

8 CJEU, 6 October 2009, C-501/06 *GlaxoSmithKline Services Unlimited v Commission and Others,* ECLI:EU:C:2009:610, para 63.

9 G. Monti, 'Excessive pricing: Competition Law in Shared Regulatory Space'. Available at: https://www.tilburguniversity.edu/sites/default/files/download/Monti%20Excessive%20pricing.pdf.

mantra that it is for data protection legislation to deal with data protection and privacy concerns and recognized that the level of data protection offered to platform users was an element of the overall quality of the product.[10]

(16) Moreover, at national level, there have been ambitious developments applying competition law to digital platforms. The German Competition Authority (the *Bundeskartellamt* – BKartA) initiated proceedings against Facebook for an alleged abuse of dominance. The BKartA claim is that Facebook is dominant on the market for social network services in Germany and that it abused its dominance on that market. In order to obtain access to the Facebook platform, Facebook users were required to consent to the processing of their data by the Facebook 'family' of applications (including Instagram and WhatsApp) and by other third party websites. This data could then be integrated with the data processed by Facebook. The BKartA considered that this practice infringed data protection law and that this infringement constituted an abuse.

(17) This finding was appealed to the OLG (Higher Regional Court) Düsseldorf, which found in Facebook's favour and overturned the preliminary decision. On appeal, the *Bundesgerichtshof* (BGH) upheld the finding of the BKartA albeit with different reasoning. Significantly, it upheld the BKartA's market definition and the data unbundling remedy proposed. The BGH did not rely directly on secondary data protection legislation to find an abuse but instead insisted on the sovereignty of consumers on the market and the link between this concept and the constitutionally protected right to 'informational self-determination'. Given that the right to data protection in the EU Charter is also founded on the notion of informational self-determination, the judgment provides an important affirmation of the importance of consumer sovereignty in digital markets in the face of digital asymmetry that is also of relevance at EU level. The remedy proposed by the BGH was, in essence, to give the consumer the choice between a free of charge service whereby Facebook could combine data acquired by Facebook family members or third-party websites with Facebook account data, and a service where the privacy sensitive consumer could pay instead.

(18) Nevertheless, despite these important developments in Competition law, the question remains whether such consumer sovereignty and associated fundamental rights (informational self-determination; autonomy and dignity) can be sufficiently protected by competition law or whether ex ante regulation is appropriate. We suggest that Competition law is insufficient for a number of reasons. First, competition law rules apply ex post and are necessarily slow in their application. As such, they can only address problems in digital markets after the fact and in specific cases, when what may

10 Commission Decision 2016/C 388/04 *Microsoft/LinkedIn* (Case M.8124), OJ 2016, C 388/04, para 350.

be required is contemporaneous intervention that is of general rather than specific application. This is implicitly recognized, for instance, in the CMA report on online platforms which recommends the creation of a 'pro-competition' regulatory regime that would help to overcome barriers to entry and expansion in digital platform markets, thus tackling sources of market power and promoting innovation.[11]

(19) Second, as the EU already noted in 2015, the way in which a number of online platforms use their market power 'raise[s] a number of issues that warrant further analysis beyond the application of competition law in specific cases'.[12] While concerns that are labelled 'non-competition concerns', such as data protection and environmental protection, can be shoehorned into the consumer welfare standard to be taken into account in competition law assessments, this piecemeal approach is necessary but not sufficient. The EU's commitment to respect and promote the values set out in the EU Charter necessitates the adoption of an ex ante regulatory instrument that is not only 'pro-competition' but that also proactively ensures consumer sovereignty in the face of digital asymmetry and ensures that the private sphere promotes collective values, including dignity, autonomy and respect for fundamental rights.

b) Market definition

(20) Pursuant to competition law, additional (or 'special') responsibilities are placed on undertakings that occupy a position of dominance or significant market power (SMP) within a market defined on the basis of established 'market definition' principles.[13] Yet, despite the pivotal importance of market definition for competition law, concerns are voiced that the market definition exercise is ill-suited to digital markets and incapable of reflecting the actual dynamics of competition in these markets.[14] We could highlight two primary concerns for present purposes.

(21) First, when defining a relevant market for product or services, the European Commission focuses primarily on demand-side substitutability, that is the extent to which consumers view products and services as interchangeable.[15] In order to measure such demand-side substitutability, a price-centric test – called the SSNIP test – is used.

---

11 Competition and Markets Authority, 'Online platforms and digital advertising', Market study final report, 1 July 2020 ('the CMA Report').

12 Commission's Communication, 'A Digital Single Market Strategy for Europe' COM(2015) 192, 12.

13 European Commission, 'Commission Notice on the definition of relevant market for the purposes of Community competition law', OJ 1997, C 372/5.

14 N. van Gorp and O. Batura, *Challenges for Competition Policy in a Digitalised Economy* (European Parliament – DG for Internal Policies, IP/A/ECON/2014-12, 2015), 50.

15 Commission Notice on the definition of relevant market for the purposes of Community competition law [1997] OJ 372/5, paras 13 and 14.

This gauges whether consumers would switch between products in the event of a small but significant non-transitory increase in prices (a price increase of 5-10%). However, given that digital markets often involve products or services that are offered for free at the point of access to consumers, such price-based assessments become meaningless.

(22) Second, this problem of gauging demand-side substitutability based on pricing assessments is further complicated by the two- or multi-sided nature of digital platforms. On these markets there are more than one set of 'consumers' and more than one 'price' offered. The price on one side of the market (most commonly, for targeted advertising) subsidises the price on the 'free' side of the market where end-users are offered the service (for instance, search engine services).

(23) Third, competition authorities have struggled to reflect accurately the role of data in market definition. Here we could note that where data is not directly traded but is used as an input for other products, there is a reluctance to acknowledge a relevant data market. In important digital mergers such as Google's acquisition of DoubleClick and Facebook's acquisition of WhatsApp, the European Commission treated data only as an input in markets where it was already being used.[16] This perspective overlooks the fact that the data acquired (from WhatsApp and Doubleclick respectively) could be used by Facebook and Google as useful input for the myriad of other data-informed services that they offer.[17]

(24) Moreover, there is often an assumption that data are fungible. However, there are a number of shortcomings to this assumption. Primarily, it downplays the market significance of data concentration by overlooking that the mere availability of this data to other entities overlooks that 'there may be different legal frameworks applicable to the different actors, limiting their ability to reuse the data', thereby imposing constraints on them.[18]

(25) As a result of these challenges, several proposals for reform have been made. For instance, the Special Advisors' report acknowledges the blurred boundaries between markets in the digital world and that the interdependence between sides of the market is critical to the analysis of market definition. The report therefore suggests that in

---

16 In Facebook/WhatsApp, for instance, the Commission did not define a market for data as neither of the entities was active on the market for the provision of data, see Case COMP/M.7217, *Facebook/ WhatsApp*, para 72.

17 Esayas, for instance, argues that it is necessary to recognise a distinct market for input data, see Esayas, n 7, 128-133.

18 Esayas, n 7, 134; Autorité de la Concurrence and Bundeskartellamt, Joint Report *Competition Law and Data*, 10 May 2016, 54.

digital markets less emphasis should be placed on the analysis of market definition and more on theories of harm and the identification of anti-competitive strategies.[19]

2. *General EU consumer law*

(26) Currently, the only special EU legislation for online platforms is Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services; which however does not apply to business to consumer relationships.[20] At best, it can be drawn upon to derive ideas about fairness and transparency generally.

(27) The so-called Omnibus Directive 2019/2161/EU[21] was the first legislative act to address certain specific consumer protection issues related to 'online marketplaces', but it did not bring about comprehensive regulation of the platform – consumer relationship. In particular, it does not contain rules on access to online marketplaces or on the price to be paid, nor does it deal with the quality of the service. Instead, it only aims to establish a certain amount of clarity on who the consumer's contracting partner is and, where it is a third party, whether this third party is a trader.[22]

(28) What remains is general consumer law, such as the Unfair Contract Terms Directive 93/13/EEC[23], the E-Commerce Directive 2000/31/EC[24] and the Consumer Rights Directive 2011/83/EU[25] that provide for certain consumer rights against platform service providers to whom the consumer is connected via a platform contract.

(29) The platform contract is a service contract by which the service provider grants access to the platform and potentially additional services.[26] Every use of a platform includes the (potentially tacit) conclusion of a platform contract, regardless of whether the user

---

19 J. Cremer, Y. Montjoye and H. Schweitzer, *Competition policy for the digital era: Final Report* (European Commission, Luxembourg), April 2019 ('The Special Advisors' Report').

20 Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services OJ 2019, L 186/57.

21 OJ 2019, L 328/7.

22 See new Article 6a of the Consumer Rights Directive 2011/83/EU.

23 OJ 1993 L 95/29.

24 OJ 2000 L 178/1.

25 OJ 2011 L 304/64.

26 See P. Rott, 'Die vertragsrechtliche Position des Online-Plattformbetreibers als Vermittler', in P. Rott and K. Tonner (eds), *Das Recht der Online-Vermittlungsplattformen* (Nomos, Baden-Baden, 2018), 62, 66 ff.

(consumer) has to register or pay a price.[27] In any event, the user 'pays' by providing his or her personal data (see also infra, IV. 4. b).[28]

(30) As the platform contract will be concluded electronically, the provisions of Directive 2011/83/EU on distance selling contracts apply. Thus, the platform service provider is obliged to give the consumer information, and the consumer has a right of withdrawal (which does not help him greatly). The platform service provider also has certain obligations under the Electronic Commerce Directive 2000/31/EC. None of these, however, relate to access to a platform, or protection against suspension or termination of the platform contract, thus exclusion from the platform, or to the affordability of the platform service.

(31) What is more useful is the Unfair Contract Terms Directive 93/13/EEC (as implemented by the Member States), at least once a platform service contract has been concluded. In particular, the Unfair Contract Terms Directive allows the control of terms related to the suspension or termination of the platform contract. Indeed, in Germany there have been numerous recent cases turning on the potential unfairness of such a term, or its correct interpretation by the platform service provider. Decisions mainly relate to Facebook but there have also been decisions concerning Youtube and PayPal. Most decisions concern (previously) existing contractual relationships (accounts), which are temporarily blocked or terminated or within which individual posts or videos of users are deleted. The platforms thereby usually rely on their standard terms, according to which they can, for example, delete posts and ban accounts if the user engages in hate speech.[29] Indeed, in the German context digital players are required by law to block and delete hate speech.[30] That case law, however, integrates the consideration of the fundamental right to free speech. It is therefore discussed below, in the context of fundamental rights law.

---

27 See also J. Sénéchal, 'The Diversity of the Services provided by Online Platforms and the Specificity of the Counter-performance of these Services – A double Challenge for European and National Contract Law', *Journal of European Consumer and Markets Law* 2016, 39, 43.

28 See LG Munich I, 25 October 2006, 30 O 11973/05, Computer und Recht 2007, 264. See also C. Wendehorst, 'Platform Intermediary Services and Duties under the E-Commerce Directive and the Consumer Rights Directive', *Journal of European Consumer and Markets Law* 2016, 30, at 31. For Austria, see the Austrian Supreme Court (Oberster Gerichtshof; OGH), 16 April 2009, 2 Ob 137/08y.

29 See also M. Beurskens, 'Hate-Speech" zwischen Löschungsrecht und Veröffentlichungspflicht', *Neue Juristische Wochenschrift* 2018, 3418, 3420. See also the joint action of national authorities against Airbnb's standard term allowing the unilateral change of the service fee in the framework of the old CPC Regulation (EC) No. 2006/2004, see the Common position of national authorities within the CPC Network concerning the commercial practices and the terms of service of Airbnb Ireland, available at https://ec.europa.eu/info/sites/info/files/final_common_position_on_airbnb_ireland_4.6.2018_en_002.pdf, 8.

30 See § 3 para. 2 *Netzdurchsetzungsgesetz* (Network Enforcement Act; NetzDG).

(32) Unfair contract terms law can also serve to control terms that allow the trader to modify the price[31] or the quality of the service in an existing contract. In relation to online platforms, this allows courts to control terms that allow the platform service provider to change the conditions for accessing the platform, for example in relation to the consumer's consent to the transfer of data to other traders. In fact, the *Kammergericht* Berlin declared Facebook's term allowing exactly that to be unfair in the terms of § 307 para. 1 BGB, the German implementation of Article 3 Unfair Contract Terms Directive.[32]

(33) A term may also be unfair if it allows the trader to modify the content of its service. For example, the pay TV provider Sky used a term that allows Sky to change or limit the programme that customers can access. On that basis, it removed Formula One races from its programme in 2018 and rejected the termination of the contract that customers demanded as they had bought a subscription precisely to watch Formula One races. The LG Munich decided that the term was too broad and therefore unfair, as it allowed Sky to change the character of its service.[33]

(34) Finally, the transparency control that is enshrined in unfair contract terms law serves to control terms that allow for the use and transfer of data that is described in a way by which the consumer cannot understand easily what will happen to his or her data. Again, German case law provides for examples.[34]

(35) In contrast, unfair contract terms law is of no help where the trader denies the consumer a contract, and it is equally unhelpful when it comes to the price, or remuneration, for the platform service, as unfair terms control does not relate to price or remuneration, according to Article 4(2) Unfair Contract Terms Directive. Moreover, unfair contract terms law does not prevent lock-in effects arising from practical difficulties of switching to another provider (on which see also infra, at IV. 3. c),

(36) Unfair commercial practices law has also been used against powerful platforms. For example, national authorities have launched a joint action under the old Consumer Protection Cooperation Regulation (EC) No. 2006/2004 against Airbnb, challenging among others price information on its website and the lack of identification of traders and commercial content.[35]

---

31 See only ECJ, 21 March 2013, Case C-92/11 *RWE Vertrieb AG v Verbraucherzentrale Nordrhein-Westfalen eV*, ECLI:EU:C:2013:180. See also the Common position of national authorities concerning Airbnb, n 29, 8.

32 KG, 20 December 2019, 5 U 9/18, *MultiMedia und Recht* 2020, 239.

33 LG Munich, 17 January 2019, 12 O 1982/18, *MultiMedia und Recht* 2019, 856. The case is pending on appeal.

34 See, for example, LG Berlin, 19 November 2013, *MultiMedia und Recht* 2014, 563, 565 – *Google*; LG Berlin, 30 April 2013, *Neue Juristische Wochenschrift* 2013, 2605, 2606 – *Apple.* For details, see P. Rott, 'Data protection law as consumer law – How consumer organisations can contribute to the enforcement of data protection law', *Journal of European Consumer and Markets Law* 2017, 113 ff.

35 See the Common position of national authorities n 29, 1 ff.

(37) In contrast, unfair commercial practices law has never been used to allow consumers access to platform services. Moreover, until recently, the Unfair Commercial Practices Directive 2005/29/EC has not foreseen individual remedies but only collective action by consumer organizations or public authorities. This will only change with the implementation of the so-called Omnibus Directive (EU) 2019/2161, which has introduced a new Article 11a to the Unfair Commercial Practices Directive, according to which consumers harmed by unfair commercial practices shall have access to proportionate and effective remedies, including compensation for damage suffered by the consumer and, where relevant, a price reduction or the termination of the contract.

(38) The Digital Content and Services Directive (EU) 2019/770, finally, only deals with digital content and services that are not in conformity with the contract, including certain update obligations of the trader, but not with issues of access or affordability of such services.

(39) In conclusion, general EU consumer law offers a certain amount of protection to consumers in existing contractual relationships but it does not guarantee affordable access to platform services. Moreover, just like competition law, it only offers *ex post* consumer protection. One telling example is the collective action of the German consumer organisation *Verbraucherzentrale Bundesverband* (vzbv) against Facebook, which has been initiated in 2013, with a first instance court decision of October 2014[36] and an appeal court decision of September 2017,[37] and which the *Bundesgerichtshof* has in May 2020 referred to the Court of Justice to clarify the legal standing of vzbv in relation to data protection law.[38]

3. *EU fundamental rights law*

(40) The sheer power of certain online platforms, in particular of Facebook, has initiated a discussion, and even litigation at the national level, concerning the question of whether powerful online platform service providers are bound by fundamental rights, such as the rights to free speech and equality. The role digital platforms play in moderating speech, by blocking accounts and deleting posts for contravention of private terms of service, has led to increased debate about this issue. Moreover, political attention is increasingly focused on systemic issues such as disinformation and the dissemination of illegal speech (ranging from terrorist content to defamatory

---

36 LG Berlin, 28 October 2014, 16 O 60/13, *Verbraucher und Recht* 2015, 110.

37 KG, 22 September 2017, 5 U 155/14, *Zeitschrift für Datenschutz* 2018, 118.

38 BGH, 28 May 2020, I ZR 186/17, *Gewerblicher Rechtsschutz und Urheberrecht* 2020, 896; registered as Case C-319/20 *Facebook Ireland*.

materials). Consequently, beyond the reform of rules on intermediary liability exemptions, whether and how fundamental rights apply to digital platforms is now being discussed. This application comes in various legal disguises: the indirect effect of fundamental rights through a fundamental rights informed application of consumer law, and the direct of fundamental rights between online platform service providers and (potential) users.

a) The indirect effect of fundamental rights

(41) As mentioned above, the issue of the indirect impact of fundamental rights by way of the interpretation of unfair contract terms law has already found the way to national courts. Users of Facebook accounts in particular, but also of the video platform Youtube, whose posts were deleted or whose accounts were temporarily blocked or even deleted due to alleged 'hate speech' or 'fake news' point to their fundamental right of free speech, which is protected under Article 5 paragraph 1 German Basic Law (Grundgesetz; GG), and authors have warned against so-called 'overblocking'.[39]

(42) All judgments of German courts have confirmed Facebook's right to sanction hate speech as well as the validity of the related standard terms as being fair as well as sufficiently transparent. At the same time, the courts have also required Facebook to consider the user's fundamental right to free speech when *applying* their standard terms. For example, the LG Bamberg came to the conclusion that, in the light of Article 5 paragraph 1 GG, a particular Facebook post (dealing, among others with illegal immigration) did not meet the standard of hate speech that allows Facebook to delete the post.[40] Similarly, in a case involving a Youtube video the KG Berlin held that, in the light of the right to free speech, the video in question did not represent hate speech. Therefore, Youtube had no (contractual) right to take it down.[41] Courts have, however, argued that private parties do not need to comply with the right to free speech in the same way as the State has to do, as long as constitutional values are observed and the decision is not arbitrary.[42] Notably, other courts have applied the principle of equality to local (rather than national or even global) power positions. In a decision of August 2020, the AG Memmingen declared that women must be allowed to participate in a local fishing competition, organised by a private association, that has traditionally been

---

39 See, e.g., B. Holznagel, 'Overblocking durch User Generated Content (UGC) - Plattformen: Ansprüche der Nutzer auf Wiederherstellung oder Schadensersatz?', *Computer und Recht* 2018, 369 ff.; A. Schiff, 'Meinungsfreiheit in mediatisierten digitalen Räumen', *MultiMedia und Recht* 2018, 366 ff.

40 *See* LG Bamberg, 18 October 2018, 2 O 248/18, *MultiMedia und Recht* 2019, 56.

41 *See* KG Berlin, 22 March 2019, 10 W 172/18, 9590 *Beck-Rechtsprechung* (2019).

42 See OLG Karlsruhe, 28 February 2019, 6 W 81/18, *Beck-Rechtsprechung* 2019, 7615; LG Heidelberg, 28 August 2018, 1 O 71/18, *Zeitschrift für Urheber- und Medienrecht – Rechtsprechungsdienst* 2019, 72. For an advocate of different standards see also J. Lüdemann, 'Grundrechtliche Vorgaben für die Löschung von Beiträgen in sozialen Netzwerken', *MultiMedia und Recht* 2019, 279 ff.

reserved to men. The court argued that the association was in a social power position locally.[43]

(43) The approach of considering fundamental rights in the application of private law is also known to other Member States[44] and to EU law. For example, in the unfair contract terms law case of *Macinský*, Advocate General Wahl considered the right to housing of Article 7 of the Charter of Fundamental Rights in his assessment of the unfairness of a term.[45] In the same way, the Court of Justice confirmed in *Kušionová* that '(u)nder EU law, the right to accommodation is a fundamental right guaranteed under Article 7 of the Charter that the referring court must take into consideration when implementing Directive 93/13.'[46]

(44) Another fundamental right that could be taken into account in the application of unfair contract terms law is the right to equality as enshrined in Article 3 para. 1 GG and Article 20 of the Charter. In Germany, this question is currently pending before the *Bundesverfassungsgericht* in another Facebook case. The case relates to the account of the right-wing party 'Der III. Weg'. Because of a post that Facebook classified as hate speech, Facebook first blocked the account for 30 days, then deleted it. 'Der III. Weg' took action in the civil courts and finally before the *Bundesverfassungsgericht*, their main line of argument asserting a violation of the principle of equality. The *Bundesverfassungsgericht* has not yet taken a final decision but, in the fast-track procedure for interim decisions, it did not exclude that Facebook might be bound by the principle of equality. It accepted the application for interim judicial protection because the ban deprived the applicant of an essential communication channel with potential voters in the critical phase before the elections to the European Parliament.[47]

b) Direct effect of fundamental rights

(45) More could be achieved if consumers, or citizens, had a directly applicable fundamental right to equality that State-like platform operators had to observe. Such a right would extend to the decision on the conclusion of a contract, thus on access to the platform, and it would prohibit the platform operator from exercising its discretion to deny an interested consumer access.

---

43 AG Memmingen, 31 August 2020, 21 C 952/19.

44 See, for example, C. Mak, Fundamental rights in European contract law. A comparison of the impact of fundamental rights on contractual relationships in Germany, the Netherlands, Italy and England (Kluwer Law International, 2008).

45 AG Wahl, 21 November 2013, Case C-482/12 *Peter Macinský, Eva Macinská v Getfin s.r.o., Financreal s.r.o.*, ECLI:EU:C:2013:765, para. 82.

46 ECJ, 10 September 2014, Case C-34/13 *Monika Kušionová v SMART Capital a.s.*, ECLI:EU:C:2014:2189, para 65.

47 *See* BVerfG, 22 May 2019, 1 BvQ 42/19, *Neue Zeitschrift für Verwaltungsrecht* 2019, 959 ff., with a case note by M. Seyderhelm.

(46) Whether or not the fundamental right to equality applies to platforms like Facebook is a hotly debated topic in Germany. The debate was fuelled by a decision of the *Bundesverfassungsgericht* that obliged the German football association to observe the right to equality when deciding on the ban of a football fan from Bundesliga matches. The *Bundesverfassungsgericht* argued that where a private actor offers goods or services to the public at large and makes far-reaching decisions on the participation of others in social life. In this situation, private players must not exclude others arbitrarily from access to their goods or services.[48] Subsequently, authors have transferred the logic of the *Bundesliga* judgment to the digital world,[49] and German courts have begun to apply fundamental rights rhetoric to powerful digital players but there has been no decision yet that confirmed a direct (rather than indirect) effect of fundamental rights in relations between a powerful platform and a consumer.

(47) The same could be considered at the EU level. After some controversial debate concerning the existence of a direct effect of the Charter of Fundamental Rights, the Court of Justice has confirmed in several cases that Charter rights can take direct effect between private parties. In *Association de médiation sociale*, the Court denied direct effect to Article 27 of the EU Charter which provides for the workers' right to information and consultation within the undertaking (because it considered that provision to be too unspecific). However, on the other hand it *obiter* maintained that the principle of non-discrimination on grounds of age, laid down in Article 21(1) of the EU Charter, was sufficient in itself to confer on individuals an individual right which they may invoke as such.[50] In the case of *Egenberger*, the Court confirmed this finding on Article 21(1), this time concerning non-discrimination on grounds of religion.[51] It added that Article 47 EU Charter on the right to effective judicial protection was also sufficient in itself and that national courts were required to ensure, within their jurisdiction, judicial protection for individuals flowing from Articles 21 and 47 and to guarantee the full effectiveness of those articles by disapplying any contrary provision of national law where necessary.[52] In *Max Planck Gesellschaft*, the Court recognised the direct effect between private parties of the right to paid annual leave, as laid down in Article 31(2) of the Charter, noting that the right of every worker to paid annual

---

48 *See* BVerfG, 11 April 2018, 1 BvR 3080/09, *Neue Juristische Wochenschrift* 2018, 1667 ff.

49 *See* A. Peukert, 'Gewährleistung der Meinungs- und Informationsfreiheit in sozialen Netzwerken', *MultiMedia und Recht* 2018, 575. For an early contribution, see K.-H. Ladeur, 'Ausschluss von Teilnehmern an Diskussionsforen im Internet - Absicherung von Kommunikationsfreiheit durch „netzwerk-gerechtes" Privatrecht', *MultiMedia und Recht* 2001, 787 ff.

50 CJEU, 15 January 2014, Case C-176/12 Association de médiation sociale v Union locale des syndicats CGT and others, ECLI:EU:C:2014:2, para. 47.

51 CJEU, 17 April 2018, Case C-414/16 *Vera Egenberger* v. *Evangelisches Werk für Diakonie und Entwicklung eV*, ECLI:EU:C:2018:257, para. 76; confirmed by CJEU, 6 November 2018, joined Cases C-569/16 and C-570/16 *Stadt Wuppertal* v. *Maria Elisabeth Bauer* and *Volker Wilmeroth* v. *Martina Broßonn*, ECLI:EU:C:2018:871, paras 85 ff.

52 CJEU - *Egenberger*, *supra* note 50, 78 f.

leave entails, by its very nature, a corresponding obligation on the employer.[53] Whether a Charter right is capable of taking direct effect between private parties depends on the individual Charter right in question.[54]

(48) According to Article 20 of the Charter, everyone is equal before the law. The principle of equality before the law is a general principle of EU law which, according to the established case law of the Court of Justice, requires that comparable situations should not be treated differently and that different situations should not be treated in the same way, unless such different treatment is objectively justified. A difference in treatment is justified if it is based on an objective and reasonable criterion, that is, if the difference relates to a legally permitted aim pursued by the legislation in question, and it is proportionate to the aim pursued by the treatment.[55] Whether or not the right to equality is among those Charter rights that can take direct effect between private parties has not been decided yet by the Court.

(49) Although one could argue that the fundamental right to equality is capable of allowing consumers to enforce access to platform services offered by powerful platform operators,[56] this is certainly a thorny road. Leaving aside legal uncertainty, each consumer would have to initiate legal proceedings in court, possibly up to a constitutional court where there is one in the relevant Member State. Thus, even where fundamental rights do offer protection to individuals in the face of digital asymmetries of power, relying on fundamental rights alone is not a practicable solution for the problem at hand. Such a solution would be costly, fragmented across Member States, and it would rely on the initiative of affected individuals.

4. Data Protection

a) General Overview

(50) The EU data protection regime is a combination of primary and secondary law measures. The protection of personal data is recognised as a fundamental right, independently of the right to respect for private life, protected by the EU Charter. Debate persists about the precise meaning, or 'added value', of this right alongside the

---

53 CJEU, 6 November 2018, Case C-684/16 *Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V.* v. *Tetsuji Shimizu***,** ECLI:EU:C:2018:874, para. 79.

54 AG Cruz Villalón, 18 July 2013, Case C-176/12 *Association de médiation sociale* v *Union locale des syndicats CGT and others*, ECLI:EU:C:2013:491, para. 38.

55 See only CJEU, 10 November 2016, Case C-156/15 *Private Equity Insurance Group SIA* v. *Swedbank AS*, ECLI:EU:C:2016:851, para. 49.

56 See the detailed analysis by P. Rott, 'Powerful Private Players in the Digital Economy: Between Private Law Freedoms and the Constitutional Principle of Equality', *Baltic Yearbook of International Law* 2020, forthcoming.

right to privacy.[57] Some suggest that the right to data protection is simply a right to a legal framework governing personal data processing.[58]

(51) More specifically, some consider that the right ensures a system of checks and balances or data governance with the aim of ensuring the fairness of data processing operations.[59] For others, data protection seeks to promote individual control over personal data, or informational self-determination, albeit recognising that such control is not, and should not be, absolute. Across these various visions, there is widespread consensus that the right to data protection, and the legislative framework that gives expression to this right, seek to enable and protect a wider range of rights, including non-discrimination, freedom of expression, dignity and autonomy.[60] In addition to the EU Charter right, Article 16 TFEU now affirms the right to data protection but also provides an explicit legislative basis for the EU in this area, thereby liberating data protection law from its internal market origins.[61]

(52) A modernised data protection law, the General Data Protection Regulation (GDPR) entered into force two years ago. This legal framework legitimises personal data processing provided that its regulatory scheme is respected: those responsible for personal data processing (controllers) must have a legal basis for processing, respect core data protection principles and remain accountable for their actions while rights are granted to individuals over their personal data.

(53) The potential of this legal framework has not yet been maximised. Public enforcement remains limited while private enforcement remains costly and lengthy.[62] Moreover, although the GDPR recognises the possibility of representative action on behalf of individuals or groups without their mandate, few EU Member States have availed of this possibility as of yet[63] while representative actions with the mandate of the data

---

57 G. Fuster and H. Hijmans, 'The EU rights to privacy and personal data protection: 20 years in 10 questions', International Workshop Exploring the Privacy and Data Protection connection: International Workshop on the Legal Notions of Privacy and Data Protection in EU Law in a Rapidly Changing World (Brussels, 2019).

58 L. Dalla Corte, 'A right to a rule: On the substance and essence of the fundamental right to personal data protection', in D. Hallinan, R. Leenes, S. Gutwirth and P. De Herts (eds), *Data protection and privacy: Data protection and democracy* (Hart Publishing, 2020), 27.

59 H. Hijmans, The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU (Springer, 2016), 62-66.

60 Text of Regulation; see also Article 35 GDPR.

61 O. Lynskey, *Foundations of EU Data Protection Law* (Oxford University Press, Oxford, 2015).

62 Commission's Communication, 'Data protection as a pillar of citizens' empowerment and the EU's approach to digital transition - two years of application of the General Data Protection Regulation' COM(2020) 264; J. Ryan, 'Europe's governments are failing the GDPR: Brave's 2020 report on the enforcement capacity of data protection authorities', Brave Browser, April 2020.

63 O. Lynskey, 'General Report Topic 2: The New EU Data Protection Regime' in J. Rijpma (ed.), *The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection* (Eleven International Publishing, 2020), 23.

subject have been plagued with procedural impediments.[64] From a substantive perspective, key aspects of the legal regime have not yet been brought to bear on digital services, including the principles of purpose limitation; data minimisation and fairness. Therefore, the data protection framework has a potentially important role to play in tackling digital asymmetry of power to the benefit of consumers and society more broadly.[65]

b) Information Requirements

(54) When it comes to information-provision requirements, transparency is a general principle of data protection law, set out in Article 5(1)(a) GDPR and elaborated upon in subsequent provisions.[66] These provisions specify the manner in which information should be conveyed to individuals[67], in a 'concise, transparent, intelligible and easily accessible form'[68], and other logistical aspects of the transparency obligation. The GDPR also prescribes the information that must be provided to data subjects. The information that must be provided to the individual relates to how their personal data will be used by the data controller (here, a platform) rather than broader information aspects about the service.

(55) When digital services are concerned and much of the content and service delivery is algorithmically determined, it is useful to consider to what extent insights can be gained into the factors driving such algorithmic curation. There has been much debate about whether the GDPR confers upon individuals a right to an explanation of automated decisions directed to them, with some suggesting that such a right does not exist.[69] The consensus in the academic literature is however that the information requirements it provides for (the provision of 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject') must be interpreted in a functional way.[70] This information should therefore be meaningful to the individual concerned (a human

---

64 A. Biard, 'Stepping up the Enforcement of Consumer Protection Rules', *Bureau Européen des Unions de Consommateurs AISBL* Report, September 2020.

65 O. Lynskey, Foundations of EU Data Protection Law, n 61, 76 f.

66 Articles 12-14 GDPR.

67 Under the GDPR, these rights are bestowed on 'data subjects', individuals who are identified or identifiable based on the processing of personal data.

68 Article 12(1) GDPR.

69 S. Wachter, B. Mittelstadt and L. Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', *International Data Privacy Law* 2017, 76 ff.

70 See, for instance, G. Malgieri and G. Comandé, 'Why a Right to Legibility of Automated Decision-making Exists in the General Data Protection Regulation, *International Data Privacy Law* 2017, 243 ff.; I. Mendoza and L. Bygrave, 'The Right not to be Subject to Automated Decisions Based on Profiling' in *EU Internet Law: Regulation and Enforcement* (Springer, 2017), 7 ff.; M. Kaminski, 'The Right to Explanation, Explained', 34 *Berkeley Technology Law Journal* (2019), 190 ff.

without technical expertise) and enable them to exercise their other rights in the data protection framework. As such, it includes not simply information about the functioning of an algorithmic decision-making system in general but how it determines outcomes for a particular individual.[71] However, as *Kaminski* notes, the GDPR also provides for many opportunities for more systemic oversight of algorithmic recommendations. Under Article 58(1)(e) GDPR; regulators have information forcing powers to obtain 'all information necessary for the performance of its tasks'. There are however gaps in these information requirements as further discussed below.

c) The Right to Data Portability

(56) Article 20 GDPR recognises that individuals have a right to data portability, enabling individuals to 'port' their data from one digital platform to another. Where technically feasible, this transfer is carried out automatically at the request of the individual.[72] This right was an entirely new right introduced by the GDPR but sits neatly within the bundle of rights granted to individuals over their personal data, including the right to access and delete personal data. As such, while it may promote competition and ensure economic benefits, it was primarily conceived as a tool to facilitate informational self-determination, or individual control over personal data.[73] There are therefore a number of notable differences between the way in which data portability operates as a right under data protection law, and its application as a remedy for competitive harms. The right to data portability only applies when particular legal basis in the GDPR are relied upon (contract and consent); it only provides to data 'provided' by the data subject (to the exclusion of inferred data and possibly observed data); the right only extends to personal data and may not apply where there is an interference with the rights and interests of others.[74] Moreover, the right to data portability must be invoked by the data subject and can be invoked vis-à-vis any entity that processes their personal data.

(57) By way of contrast, a data portability remedy under competition law, where an undertaking was required to provide access to data to other economic entities for instance, could be crafted in a way that is simultaneously narrower and broader. Such a remedy might be more narrow in so far as it would only apply to certain market actors (those with a dominant position, for instance) and broader in that it could encompass

---

71 A.D. Selbst and J. Powles, 'Meaningful information and the right to explanation', *International Data Privacy Law* 2017, 233, 236.

72 Article 20(3) GDPR.

73 O. Lynskey, 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability', *European Law Review* 2017, 793 ff.

74 These limitations follow from the text of Article 20 GDPR. For Guidance on how they may apply in practice see: Article 29WP, Guidelines.

personal and non-personal data, would not be dependent on the initiative of any one individual and would not be constrained by limitations such as those relating to the legal basis for original data processing.[75] It is also worth noting that the GDPR facilitates 'one-off' transfers of data between data controllers, such as platforms, but it does not facilitate the transfer of this data on an on-going basis.[76]

(58) Looked at in the context of digital platforms, the GDPR right can therefore enable consumers to move their data between platforms. However, in the absence of a competitive market with a variety of options for consumers to choose from, this may not be a particularly useful right.[77] For instance, if a social media user chooses to no longer use Instagram to share photos with friends and followers, portability enables the user to leave Instagram without foregoing their photos; however, it does not help them communicate with others who still use the Instagram platform.

(59) In order to foster more competition on the market, more far-reaching regulatory interventions are necessary depending on the market at issue. The two most obvious are access related and discussed below.

(60) It is also worth noting that should tools such as digital assistants acquire a more prominent role in our lives, further regulatory intervention might be required to ensure use choice. A digital assistant cannot by its nature, for instance, stream content simultaneously, and thus a limitation of choice is inherent in the nature of the service offered. Some have suggested that a 'fiduciary duty of the digital assistant towards its owner' might be necessary as a result.[78]

d) Limits on Data Monetisation

(61) The GDPR does not expressly prohibit or even note the dominant online practice of data monetisation. However, it could potentially impose limits on this practice in a number of ways. If the legal basis relied upon for personal data processing is consent or that processing is necessary to enter into or perform a contract, both lead us to question whether the extent of the data processing is strictly *necessary.* The EDPB does not consider that 'contract' can justify data processing for advertising monetisation purposes. It states that:

---

75 See further Lynskey, n. 73 above.

76 The Special Advisors' Report, n 19, 81.

77 It is for this reason that several recent reports on competition in the digital economy conclude that the GDPR right alone will be insufficient to foster enhanced competition in digital platform markets. See, eg. The Special Advisors' Report, at 82 which states that '[a]rguably, a more stringent data portability regime can be imposed on a dominant firm in order to overcome particularly pronounced lock-in effects.'

78 The Special Advisors' Report, n 19, at 64.

> Although such processing may support the delivery of a service, it is separate from the objective purpose of the contract between the user and the service provider, and therefore not necessary for the performance of the contract at issue.[79]

(62) Under Article 7(4) GDPR, in assessing whether consent is 'freely given' utmost account must be taken of whether the performance of the contract is made conditional on 'unnecessary' data processing. Data protection authorities have not yet paid much attention to this criterion.[80]

(63) Despite these affordances under data protection law, it is also important to recognise its limits. We might classify data protection as relational to a large extent. It governs relationships between individuals (data subjects) and digital service providers (data controllers). While it can shape the way in which such data controllers process personal data and, to a limited extent, design their data processing systems, more regulatory remedies are not available to data protection authorities.[81] In this way, while the framework can enable individuals to exercise their rights and some data processing practices can, for instance, be banned or suspended, data protection law cannot force ongoing structural change to ensure that the data subject is offered a choice between different forms of data processing practices (a 'choice architecture' to the benefit of the data subject). It can support the right to data portability, for example, but not require infrastructural changes to support interoperability. Equally, it can sanction excessive or exploitative data processing practices but not mandate the provision of suitable alternatives for the individual.

5. Interim observations

(64) The legal frameworks for competition law, data protection and consumer protection as well as the protection of fundamental rights offer individuals some protection in the face of digital asymmetries of power. Nevertheless, there are gaps in this protection, primarily due to the ex post and often case-specific application of these legal frameworks, that could be filled by the introduction of an ex ante legal framework.

III. Possible Policy Avenues

(65) Given the observed shortcomings of the current legal framework, different possible policy avenues can be thought of, in particular a public or constitutional law approach

---

79 European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, adopted on 8 October 2019, 15.

80 For a discussion of some of the national decisional practice on this issue see Lynskey, n 61, 45-47.

81 Article 25 GDPR.

and an ex-ante regulation approach that has an economic focus drawing on competition law concepts. In contrast, we propose an approach anchored in the law on services of general interest, as applied by the EU in areas such as energy supply, telecommunications services and basic bank accounts.

1. Public or constitutional law approach

(66) In recent years, there has been much debate about the constitutionalisation of platforms, including obliging them to respect fundamental rights, such as the right to free speech, and it was correctly observed that the current design of EU secondary law, and in particular the Electronic Commerce Directive 2000/31/EC hardly reflected the governing power of platforms.[82]

(67) As mentioned above, EU fundamental rights law is, in principle, capable of being applied horizontally, between private parties. This is, first of all, possible by way of considering the fundamental rights of citizens within the interpretation of EU consumer law, and in particular the Unfair Contract Terms Directive 93/13/EEC. This would allow consumers to oppose, for example, the deletion of messages and postings or the ban of their accounts based on the standard terms of platform providers, thus limiting the contractual freedom of the platform provider. It would, however, offer no protection outside an existing relationship.

(68) Access to an (unwilling) platform could then only be achieved if a horizontal effect of fundamental rights between a citizen and the platform was recognised. While this is generally possible, as shown above, the exact rights that would be recognised as having such a horizontal effect are as unclear as are the players that would be obliged to honour them.

(69) At to the latter, one could best draw from the case law of the Court of Justice in relation to obstacles to fundamental freedoms that are created by private players. Usually, such obstacles may be regarded as a violation of a fundamental freedom by the relevant Member State that would be responsible for preventing obstacles, as, for example, in the case of *Commission v. France*,[83] concerning protests by French farmers that the Republic of France has not stopped. However, the case of *Fra.bo*[84] provides

---

82 See, for example, N. Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms', *Social Media + Society* July-September 2018, 1 ff.; M. Smith, *Enforcement and cooperation between Member States – E-Commerce and the future Digital Services Act*, 2020.

83 ECJ, judgment of 9 December 1997, Case C-265/95 *Commission v France*, ECLI:EU:C:1997:595. Similarly, ECJ, judgment of 12 June 2003, Case C-112/00 *Eugen Schmidberger, Internationale Transporte und Planzüge v Austria*, ECLI:EU:C:2003:333.

84 CJEU, judgment of 12 July 2012, Case C-171/11 Fra.bo SpA v Deutsche Vereinigung des Gas- und Wasserfaches eV (DVGW) — Technisch-Wissenschaftlicher Verein, ECLI:EU:C:2012:453.

for an example where the breach of Article 34 TFEU was attributed directly to a private player.

(70) In Germany, the *Deutsche Vereinigung des Gas- und Wasserfaches eV* (DVGW) offers the only possibility to obtain a compliance certificate for copper fittings with the relevant legal requirements on water supply. In Fra.bo, DVGW had denied certification of copper fittings produced and distributed by the Italian producer Fra.bo, thereby effectively denying Fra.bo access to the German market (as almost all German consumers only buy copper fittings that have been certified by the DVGW). Although the DVGW is a private organisation, the Court of Justice treated this as an obstacle to the free movement of goods. It reasoned that the DVGW, by virtue of its authority to certify the products, in reality holds the power to regulate entry into the German market of products such as the copper fittings at issue.[85]

(71) Although the DVGW had that *de facto* power due the fact that the German legislator had entrusted the DVGW with the setting-up of standards for copper fittings, Advocate General Trstenjak did not appear to consider that delegation of power as the crucial element of the case. She emphasized that the DVGW was 'capable of erecting new barriers to the free movement of goods in the European Union when exercising that de facto power'.[86] The Advocate General thereby drew from the case law of the Court of Justice in relation to the freedom of movement for workers, the freedom of establishment and the freedom to provide services where the Court had explained that these freedoms would be compromised if the abolition of State barriers could be neutralised by obstacles resulting from the exercise of their legal autonomy by associations or organisations not governed by public law.[87]

(72) Whereas the fundamental rights of the Charter of course do not have the cross-border element of the fundamental freedoms of the TFEU, the criterion of *de facto* power appears to be transferable. That *de facto* power exists within contractual relationships, at least where there is a lock-in effect that makes it difficult to simply switch to another provider. Outside contractual relationships, it would seem to require a dominant position similar to the one that must not be abused under competition law, with the difference that 'abuse' is not a requirement but lack of respect for fundamental rights. The German *Bundesgerichtshof* recently attributed such a position to Facebook.[88] In academic writing, Youtube and Twitter have been regarded as being State-like, next to

---

85 For details, *see* H.-W. Micklitz and R. van Gestel, 'European Integration through Standardization: How Judicial Review is Breaking Down the Club House of Private Standardization Bodies', *Common Market Law Review* 50 (2013), 145 ff.

86 Advocate General Trstenjak, opinion of 28 March 2012, Case C-171/11 Fra.bo SpA v Deutsche Vereinigung des Gas- und Wasserfaches eV (DVGW) — Technisch-Wissenschaftlicher Verein, ECLI:EU:C:2012:176. para. 47.

87 ibid., para. 46.

88 See BGH, 23 June 2020, KVR 69/19, *Gewerblicher Rechtsschutz – Rechtsprechung* 2020, 20737.

Facebook,[89] and PayPal has been considered to have a dominant position in the market for online payment services.[90] Other commentators, however, pointed to the fact that the approach creates some uncertainty, not least because dominance may change over time.[91]

(73) In its decision in *Der III. Weg*, the German *Bundesverfassungsgericht* also mentioned the criteria of orientation of the platform, the degree of dependence on the platform and the interests of the platform operator and other third parties.[92] These criteria appear to be secondary in the sense that they come into play once the dominant position has been established and the balance of interest between the platform and the (potential) user must be determined.

(74) It seems, however, clear that even a codification of any sort of obligation to respect the fundamental rights of the Charter in secondary law, for example in the framework of the future Digital Services Act, would be limited to platforms with State-like power; and it would require a massive step in fundamental rights law that the EU legislator is unlikely to take.

2. Competition law approach with the Digital Markets Act

(75) As alluded to above, the recent reports on the application of competition law to digital environments, point to a number of its alleged shortcomings. Three overarching concerns might be distilled from these reports. First, that the existing conceptual tools in competition law (ranging from those used for market definition to current theories of harm) are insufficiently flexible. This concern remains vigorously contested by those defending the status quo, who argue that the proposed changes would merely serve to replace law with regulatory discretion.[93] Second, the concern is voiced that, in particular in light of the complexities of digital markets, the demanding exercise of defining the relevant market(s) and evidencing competitive harm is made more arduous for competition authorities. This in turn leads to lengthy and resource-intensive decision-making processes which are ill-suited to the fast-moving nature of digital markets. As a result, some suggest that it is desirable to introduce analytical short-cuts, such as the reversal of the burden of proof in some contexts, in order to

---

89 See U. Kischel, 'GG Art. 3', in: V. Epping and C. Hillgruber (eds.), *BeckOK Grundgesetz*, 41 ed. (C.H. Beck, 2019), at para. 93b.

90 See R. Podszun, 'Paypal kann sich für Kontosperre nicht auf Kuba-Embargo stützen', *Gesellschafts- und Wirtschaftsrecht* 2016, 211 ff.

91 See Kischel, n 89, para. 93b.

92 BVerfG, 22 May 2019, 1 BvQ 42/19, *Neue Zeitschrift für Verwaltungsrecht* 2019, 959 ff, para. 15.

93 See, for instance, P. Ibáñez Colomo, 'Protecting the "Law" in Competition Law', *Journal of European Competition Law & Practice* 2020, 333.

facilitate the work of competition authorities.[94] Finally, it is suggested that competition law is not an effective instrument to promote competition for markets, where unseating an incumbent is highly unlikely as a result of market failure, including consumer inertia, or because the market has already tipped. In other words, competition law struggles to deal with underlying structural issues where, rather than being driven by the strategic conduct of an undertaking, harm to competition is driven by the underlying economic features of these markets.[95]

(76) The Commission's proposed Digital Markets Act (DMA) offers a legislative response to some of these concerns as it seeks to ensure a fair and competitive economy through ex ante economic regulation.[96] This legislative initiative has four principal aims.[97] These are as follows:

- The promotion of competition, market contestability and innovation,
- Empowering users,
- Ensuring fairness in B2B relationships,
- Promoting the Digital Single Market.

(77) Article 1(1) DMA provides that the 'Regulation lays down harmonised rules ensuring contestable and fair markets in the digital sector across the Union where gatekeepers are present.' The proposed Regulation applies to the 'core platform services' offered by digital gatekeepers. A list of core platform services is found in Article 2(2). The criteria for designation as a gatekeeper are found in Article 3(1) with the thresholds for a rebuttable presumption for such designation found in Article 3(2) of the text. Chapter III of the proposal is concerned with gatekeeper practices that 'limit contestability or are unfair'. This Chapter sets out a number of obligations that apply automatically to the core platform services offered by gatekeepers. Of particular note in this context is the obligation to refrain from combining personal data sourced from core platform services with personal data from other gatekeeper or third-party services in the absence of GDPR-compatible consent.[98] Chapter III also sets out obligations that may require further specification. These include an obligation to refrain from technically restricting end users of the gatekeeper operating system from using software applications and services of their choice[99] and an obligation to 'allow business users

---

94 For example, the Special Advisors' Report, n 19, 71.

95 This follows from the CMA Report, which recommends the creation of a Digital Markets Unit to oversee codes of conduct applicable to digital platforms, see CMA Report, n 11.

96 Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM (2020) 842 final (the DMA proposal).

97 These aims are identified in the CERRE Report on the DMA. CERRE Recommendations Paper, 'Digital Markets Act: Making Economic Regulation of Platforms Fit for the Digital Age', November 2020, 7.

98 The DMA proposal, n 96, Article 5(a).

99 Ibid, Article 6(e).

and providers of ancillary services access to and interoperability with the same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services'.[100]

(78) One may therefore query how the SGI approach proposed in this paper relates to this current legislative initiative for a DMA. The two initiatives could potentially overlap as both the DMA and an SGI approach seek to promote market access (including by promoting competition, market contestability and innovation) and to empower users. In particular, the market access requirements of an SGI approach may lead to such overlap; the interoperability requirement in the DMA may, for instance, overlap with an interoperability requirement under an SGI approach. Where such overlap exists, the two approaches should be looked at as alternatives.

(79) Nevertheless, despite this overlap, the two approaches have distinct starting points. The DMA remains rooted in primarily economic concerns. The Commission's proposal states this clearly:

> 'the DMA proposal is concerned with economic imbalances, unfair business practices by gatekeepers and their negative consequences, such as weakened contestability of platform markets.'[101]

(80) By contrast, an SGI approach is rooted in citizens' rights and consumer protection and the recognition that the market may not deliver some social goods to users. For instance, an assessment under the DMA is likely to require some consideration of whether a practice might be justified on the grounds of economic efficiency, whereas efficiency considerations would not be (as) relevant under an SGI approach. If a service is deemed an SGI, it should be offered to users under certain conditions irrespective of whether this offer is efficient. These include positive universal service obligations on SGI providers such as affordability obligations that extend beyond the economic considerations of competition law.

(81) There are thus two possibilities. The SGI approach could act as a substitute for elements of the DMA, providing an alternative pathway to user empowerment and the promotion of market access. By pursuing this approach, treating the SGI approach as an alternative to the DMA, the Commission would avoid the imposition of overlapping regulatory obligations on entities falling within the scope of both initiatives while ensuring that the end-consumer continues to benefit from these obligations. Equally, pursuing the SGI approach could complement the approach taken by the DMA, supplementing it with universal service obligations which do not flow from the DMA itself. Article 1(5) of the DMA proposal foresees that Member States can impose

---

100 Ibid, Article 6(f).

101 Ibid, 3.

further obligations on gatekeepers if the purpose is to pursue other legitimate interests (beyond ensuring contestable and fair markets). It goes on to state that:

> In particular, nothing in this Regulation precludes Member States from imposing obligations, which are compatible with Union law, on undertakings, including providers of core platform services where these obligations are unrelated to the relevant undertakings having a status of gatekeeper within the meaning of this Regulation in order to protect consumers or to fight against acts of unfair competition.

Pursuing an SGI approach would pursue other legitimate interests, namely the protection of consumers.

3. An SGI approach

(82) Given the shortcomings of the two above-mentioned approaches, we propose the avenue of treating platform services, under yet to be determined conditions, as services of general interest (SGI). That approach allows us to combine competition law elements with the needs-based perspective of fundamental rights law but also to spell out concrete rights and obligations akin to those that have been recognised, or rather codified, in relation to other SGI.

(83) SGI are, first of all, mentioned in EU primary law, for various reasons. Historically, they have come to the fore at EU level in part because of their relationship with the Treaty provisions on competition law. In particular, various aspects of the mode of delivery of SGI and the way they may be supported by the State may raise competition law issues. There is therefore a need to decide how these issues should be balanced with the particular 'general interest' nature of the services. This balancing exercise is addressed by Article 106(2) TFEU, according to which

> (u)ndertakings entrusted with the operation of services of general economic interest or having the character of a revenue-producing monopoly shall be subject to the rules contained in the Treaties, in particular to the rules on competition, in so far as the application of such rules does not obstruct the performance, in law or in fact, of the particular tasks assigned to them.

(84) SGI, however, have progressed and partly departed from that competition law context. This, firstly, resonates in Article 14 TFEU, which reads:

> Without prejudice to Article 4 of the Treaty on European Union or to Articles 93, 106 and 107 of this Treaty, and given the place occupied by services of general economic interest in the shared values of the Union as well as their role in promoting social and territorial cohesion, the Union and the Member States, each within their respective powers and within the scope of application of the Treaties, shall take care that such services operate on the basis of principles and conditions, particularly economic and financial conditions, which enable them to fulfil their missions.

(85) The mention of services of general needs in the context of social and territorial cohesion in Article 14 TFEU points towards a citizen-oriented approach;[102] which would also be in line with the linguistic meaning of services being of interest for those who demand these services.[103]

(86) This perspective is even clearer in the communications of the European Commission. In its White Paper on services of general interest, the Commission uses human rights language when it claims that access to affordable high-quality services of general interest is an essential component of European citizenship and necessary in order to allow citizens to fully enjoy their fundamental rights.[104]

(87) Obvious candidates are water supply services, natural gas and electricity supply services, public telecommunication services, postal services, transport services and the collection and treatment of waste.[105] The EU legislator has also recently regulated access to basic bank accounts as SGI.[106]

(88) Still, it is worth noting that there are no clear criteria for what constitutes a SGI. First of all, although many SGI have been offered by the State in the past and were then liberalised, this is not a necessary ingredient of the concept. The example of basic banking shows that the concept of SGI is dynamic, and services that have been less important in the past, or even non-existent, may become of general interest due to economic or societal development. Also, broadband internet is now recognised as an SGI, whereas it was still regarded as non-essential in the last reform of EU telecommunications law in 2009.

(89) Secondly, the concept does not require a market structure where one particular supplier is dominant, as the recognition of telecommunication services as SGI demonstrates. In telecommunication services markets, there is great competition between service providers, although in some Member States a (perhaps formerly

---

102 See also H.-W. Micklitz, The Politics of Justice in European Private Law: Social Justice, Access Justice, Societal Justice (Cambridge University Press, Cambridge, 2018), 296 f.

103 On the link between services of general interest and citizenship, see also M. Friedland and S. Sciarra (eds.), *Public Services and Citizenship in European Law* (Clarendon, 1998), with contributions by G. Amato, 'Citizenship and Public Services – Some General Reflections' (C. HARLOW "Public Service, Market Ideology, and Citizenship', E. Picard. 'Citizenship, Fundamental Rights, and Public Services' and W. Sauter, 'Universal Service Obligations and the Emergence of Citizens' Rights in the European Telecommunications Liberalization'. See also M. Ross, 'The Europeanization of Public Services Supervision: Harnessing Competition and Citizenship', *Yearbook of European Law* 2004, 303 ff.

104 See European Commission, *White Paper on Services of General Interest*, COM(2004) 374, 4.

105 For more details, see P. Rott and C. Willett, 'Consumers and services of general interest' in G. Howells, I. Ramsay, T. Wilhelmssson (eds.), *Handbook of Research on International Consumer Law*, 2nd ed. (Edward Elgar, Northampton, 2018), 267 ff.

106 See Directive 2014/92/EU on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features, O.J. 2014 L 257/214. For the classification of basic banking services as SGI, see the Commission's Communication *A Quality Framework for Services of General Interest in Europe*, COM(2011) 900, 12.

State-owned) ex-monopolist may still be in a strong position. In the banking sector, responsible for making available basic bank accounts, competition is present all over the EU.

(90) The needs-oriented perspective can also be found in secondary law. According to Article 3(2) of the Postal Services Directive 97/67/EC, 'Member States shall take steps to ensure that the density of the points of contact and of the access points takes account of the needs of users.'

(91) The concept of SGI clearly encompasses services that meet *social* needs.[107] Telecommunications is one example. Moreover, the EU Commission and the Court of Justice have recognised a variety of special TV programmes as being 'services of general economic interest' (in the terms of EU competition law, namely Article 106(2) TFEU, ex-Article 86(2) EC), although State-funded broadcasting in general has always been a controversial issue.[108] Notably, Article 15(1) and (6) of the Audiovisual Media Services Directive 2010/13/EU grants access on a fair, reasonable and non-discriminatory basis to events of high interest to the public.

(92) The social dimension is also illustrated by one typical element of EU law on SGI: the so-called universal service obligations. Recital (212) of the European Electronic Communications Code describes universal service as follows: 'Universal service is a safety net to ensure that a set of at least the minimum services is available to all end-users and at an affordable price to consumers, where a risk of *social exclusion* arising from the lack of such access prevents citizens from *full social and economic participation in society*.'[109] We will return to the question of criteria for the classification of a platform service as essential after having identified what characterises SGI and their regulation under EU law.

IV. The Legal Framework applicable to SGI: A Model Ex Ante Regulation?

1. EU policy related to SGI

(93) EU law approaches SGI from multiple angles.[110] These include, in particular, the law relating to competition, subsidies and the regulation of networks; aiming to increase

---

107 See also ibid., 291.

108 See also Protocol (No. 29) on the system of public broadcasting in the Member States annexed to the TFEU.

109 Italics added.

110 See only the variety of topics discussed in M. Krajewski, U. Neergard and J. van de Gronden (eds), *The changing legal framework for SGI in Europe - Between competition and solidarity* (Asser Press, 2009).

choice in the supply markets at a regulatory level. In relation to the role of consumers, the EU pursues a twofold approach.

(94) On the one hand, the consumer shall be empowered to avail of the benefits of competition; which confirms the finding above that the concept of SGI is not necessarily linked to a powerful position in the market; but perhaps to a powerful position vis-à-vis the end consumer.

(95) On the other hand, compensating for the potential harshness of contract law, the consumer is protected through universal service obligations that are imposed on (certain) suppliers (next to general consumer law obligations). Universal service means guaranteed access for everyone, whatever the economic, social, or geographical situation, to a service of a specified quality at an affordable price. Moreover, it appears in Article 36 of the Charter of Fundamental Rights, according to which '[t]he Union recognises and respects access to services of general economic interest as provided for in national laws and practices, in accordance with the TFEU, in order to promote the social and territorial cohesion of the Union'.[111]

2. *EU secondary law*

(96) Originally, SGI were an area that Member States could regulate beyond the strict rules of EU competition law. EU secondary law related to SGI was then established to accompany the liberalization of certain economic sectors. Liberalisation of SGI at EU level started with telecommunications services in the 1980s. Liberalisation of the electricity[112] and gas[113] markets as well as the market for postal services[114] followed in the 1990s. The EU legislator has also (modestly) targeted health services[115] and, as mentioned above, basic banking. The process is ongoing, and the latest reforms of telecommunications law dates from 2018, whereas the electricity and gas market regulation was last reformed in 2019. Notably, the relevant legal changes reflect changes in market structures but also technological and societal developments; which confirms the flexibility of the concept of SGI.

---

111 For a detailed discussion of Art. 14 TFEU and Art. 36 of the Charter of Fundamental Rights, see M. Melcher, *Dienstleistungen von allgemeinem wirtschaftlichem Interesse im europäischen Privatrecht* (Mohr Siebeck, 2016), 87–108.

112 Directive 96/92/EC, OJ 1997, L l27/20, replaced by Directive 2003/54/EC, OJ 2003 L 176/37, which was then replaced by Directive 2009/72/EC.

113 Directive 98/33/EC, OJ 1998, L 204/1, replaced by Directive 2003/55/EC, OJ 2003, L 176/57, which was then replaced by Directive 2009/73/EC, OJ 2009, L 211/94.

114 See the Postal Services Directive 97/67/EC, OJ 1998, L 15/14, as amended by Directive 2002/39/EC, OJ 2002, L 176/2, and Directive 2008/6/EC, OJ 2008, L 52/3.

115 Directive 2011/24/EU on the application of patients' rights in cross-border healthcare, OJ 2011, L 88/45.

(97) The following considerations therefore mainly focus on the current framework consisting of

- Directive (EU) 2018/1972 establishing the European Electronic Communications Code;
- Directive (EU) 2019/944 on common rules for the internal market for electricity;
- Directive 2009/73/EC on common rules for the internal market in natural gas (as amended by Directive (EU) 2019/692 without impact on consumer law);
- Directive 97/67/EC on common rules for the development of the internal market of Community postal services and the improvement of quality of service, as amended by Directive 2002/39/EC; and
- Directive 2014/92/EU on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features

but they also take into account the historical development of relevant EU legislation.

3. Typical market-related rules

(98) Market-related rules first of all aim to create competition where there has been none before, for example due to state monopolies or to natural monopolies, such as ownership of the network that connects consumers with suppliers. As far as detailed rules on consumer protection have been adopted in EU secondary law, most of them aim at allowing the consumer to choose between different providers of SGI.[116]

a) Infrastructure

(99) A great deal of legislation concerning SGI is public law regulation designed to foster competition.[117] National monopolies were broken up, making competition possible. Key concepts are interconnectivity and transmission: Network providers are obliged to grant all competitors access to their network, at a fair and reasonable price;[118] which allows these competitors to supply customers.

(100) In practice, transmission fees, and also certain exemption clauses that justify denial of transmission, have proved to be major obstacles to competition between suppliers; which is, however, not the focus of this study, in which we rather explore the supplier – consumer relationship.

---

116 See P. Rott, 'Consumers and SGI: Is EC Consumer Law the Future?', *Journal of Consumer Policy* 2007, 49, 53 ff.; Melcher, n 111, 201–204.

117 See, for example, A. de Streel and C. Hocepied, 'The Regulation of Electronic Communications Networks and Services', in L. Garzaniti, M. O'Regan, A. de Streel and P. Valcke (eds), *Electronic communication, Audiovisual services and the Internet: EU Competition Law and Regulation*, 4th ed. (Sweet & Maxwell, 2019, 25, 74 ff.

118 European Commission, *Green Paper on Services of General Interest*, COM(2003) 270, 21.

b) Pre-contractual information

(101) Firstly, in order to allow for competition and choice, market transparency shall be established, which is meant to reduce the information asymmetry between the service providers and the consumers that contributes to market failures in the field of SGI. The most important tool is the pre-contractual information obligation.

(102) Examples are the detailed lists of pre-contractual information of Annex I of the Gas Market Directive 2009/73/EC, Article 10(3) of the Electricity Market Directive (EU) 2019/944 and Article 102(1) with Annex VIII of Directive (EU) 2018/1972 establishing the European Electronic Communications Code.[119]

(103) In recent legislation, consumers shall be further supported with comparison websites. For example, Article 7 of the Payment Accounts Directive 2014/92/EU requires Member States to ensure that consumers have access, free of charge, to at least one website comparing fees charged by payment service providers, and Article 103 of the European Electronic Communications Code provides for a similar requirement.

c) Right to switch

(104) The second important instrument to allow consumers to benefit from a competitive market is the right to switch supplier, which we find, for example, in Article 106(1) of the European Electronic Communications Code, in Article 12(2) of the Electricity Market Directive (EU) 2019/944 as well as in Article 9 of the Payment Services Directive 2014/92/EU.

(105) As switching supplier has often been troublesome in the past and sometimes led to temporary lack of access to relevant services altogether, EU legislation requires suppliers to support the switching process in different ways.

(106) For example, for the case of switching between providers of internet access services, Article 106(1) of the European Electronic Communications Code requires the providers concerned to ensure continuity of the internet access service, unless technically not feasible. The receiving provider shall ensure that the activation of the internet access service occurs within the shortest possible time on the date and within the timeframe expressly agreed with the end-user. The transferring provider shall continue to provide its internet access service on the same terms until the receiving provider activates its internet access service. Loss of service during the switching process shall not exceed one working day.

(107) Similarly, payment accounts service providers have to provide a switching service that is detailed out in Article 10 of the Payment Services Directive 2014/92/EU. At the

---

119 On the latter, see de Streel and Hocepied, n 117, 106 ff.

request of the consumer, the entire switching process is organised between the old and the new service provider.

d) Avoidance of lock-in effects

(108) Apart from the potential temporary loss of service, other elements can limit the right to switch of consumers, or their desire to do so.

(109) First of all, regarding long-term contracts of continuous supply, the right to choose a service provider implies that contractual terms must not limit the right to terminate an existing contract unreasonably. Therefore, the EU legislator has introduced rules on maximum contract duration in telecommunications law.[120] According to Article 105(1) of the European Electronic Communications Code:

> Member States shall ensure that conditions and procedures for contract termination do not act as a disincentive to changing service provider and that contracts concluded between consumers and providers of publicly available electronic communications services (…) do not mandate a commitment period longer than 24 months. Member States may adopt or maintain provisions which mandate shorter maximum contractual commitment periods.

(110) Another impediment that the European Electronic Communications Code has taken up is bundling. The bundling of services may prevent the consumer from switching supplier for several reasons.[121] First, the risk of temporary lack of access to services increases when several services, such as telephone, internet and television, are switched at the same time. Second, the duration of different parts of the bundle may differ, which renders their termination more difficult. Also, costs may arise for an early termination of a service where no regular termination right exists. To remedy the problem, Article 107(1) of the European Electronic Communications Code provides that if a bundle of services or a bundle of services and terminal equipment offered to a consumer comprises at least an internet access service or a publicly available number-based interpersonal communications service, the special rules on maximum contract duration and the right to switch, among others, apply to all elements of the bundle including, mutatis mutandis, those not otherwise covered by those provisions.

(111) Finally, the right to switch, even if possible, may be unattractive when it causes practical problems to the customer that outweigh the benefits. Therefore, the EU legislator has introduced accompanying rules that aim to avoid such problems. In the area of telecommunications law, in particular, a key concept to facilitate the change of

---

120 For details, see de Streel and Hocepied, n 117, 107 f.

121 See P. Rott, 'Bündelverträge aus verbraucherrechtlicher Perspektive', *Gewerblicher Rechtsschutz und Urheberrecht – Internationaler Teil* 2018, 1010 ff.

service provider is number portability, which is now regulated in great detail in Article 106 of the European Electronic Communications Code.[122]

4. *Typical universal service obligations*

(112) As mentioned above, recital (212) of the European Electronic Communications Code describes universal service as follows:

> Universal service is a safety net to ensure that a set of at least the minimum services is available to all end-users and at an affordable price to consumers, where a risk of social exclusion arising from the lack of such access prevents citizens from full social and economic participation in society.

(113) In the following, we will discuss individual elements of universal service obligations, as they appear – with variations – in EU secondary law.

a) Access

(114) The most prominent principle is access to SGI. Access has several aspects. In network industries, there is the element of the availability of a network and of physical access in terms of connection to that network; which is of course a precondition of landline access to digital platforms. In terms of contract law, the consumer's right of access to SGI limits the supplier's freedom of contract, or more precisely, their freedom not to contract with specific individuals by creating the obligation to contract. Individual pieces of EU legislation on SGI differ with regard to the addressees of such an obligation. Finally, there is the issue of continued access.

i. Obligation to contract

(115) One example of such an obligation to contract is found in Article 84(1) of the European Electronic Communications Code. It provides:

> Member States shall ensure that all consumers in their territories have access (…) to an available adequate broadband internet access service and to voice communications services at the quality specified in their territories, including the underlying connection, at a fixed location.

(116) According to Article 27(1) of the Electricity Market Directive:

> Member States shall ensure that all household customers (…) enjoy universal service, namely the right to be supplied with electricity of a specified quality within their territory at competitive, easily and clearly comparable, transparent and non-discriminatory prices.

---

122 ibid., 109.

(117) Under Article 16(2) of the Payment Account Directive, Member States shall ensure that consumers legally resident in the Union, including consumers with no fixed address and asylum seekers, and consumers who are not granted a residence permit but whose expulsion is impossible for legal or factual reasons, have the right to open and use a payment account with basic features with credit institutions located in their territory.

ii. Limits to termination of the contract

(118) Access to services also implies that contracts guaranteeing access cannot be easily terminated, or services suspended, as this would defeat the possibility to use the services to which consumers have a right to access.

(119) Thus, Article 19(2) of the Payment Accounts Directive explicitly limits the grounds that justify termination to cases of unlawful activities, non-activity (which means that the account is not needed) and fraud. In addition to that, it allows Member States to:

> identify additional limited and specific cases where a framework contract for a payment account with basic features may be unilaterally terminated by the credit institution.
>
> Such cases shall be based on provisions of national law applicable in their territory and shall be aimed at avoiding abuses by consumers of their right to access a payment account with basic features.

One such reason is non-payment of fees.

(120) The Electricity Market Directive mentions limitations of the right of termination in relation to vulnerable customers. According to its Article 28(1), Member States shall define the concept of vulnerable customers which may refer to energy poverty and, inter alia, to the prohibition of disconnection of electricity to such customers in critical times.

(121) The limitation of grounds for the termination of the contract is often combined with procedural safeguards. In the case of the Payment Accounts Directive, service providers must inform the consumer of the grounds and the justification for the termination at least two months before the termination enters into force, in writing and free of charge. They must also advise the consumer of the procedure to submit a complaint against the termination, if any, and of the consumer's right to contact the competent authority and designated alternative dispute resolution body and provide the relevant contact details.

b) Affordability

(122) Closely linked to the access to services is their affordability. Obviously, access to services remains theoretical as long as individuals are unable to afford them.[123] For

123 See also Melcher, n 111, 314.

example, Article 12 of the Postal Market Directive 97/67 explicitly requires prices to be such that all users have access to the services provided. Article 84(1) of the European Electronic Communications Code explicitly requires affordability. Article 85 of that Directive calls on Member States who find that consumers with a low income or special social needs are prevented from accessing adequate broadband internet access service and to voice communications services, to take measures to ensure affordability for such consumers of adequate broadband internet access service and voice communications services at least at a fixed location.[124]

(123) What exactly affordability means is not entirely clear, despite clarification attempts of the European Commission.[125] The Court of Justice has decided that affordability does not exclude reasonable profit on the part of the supplier.[126] At the same time, it is obvious that some SGI, in particular public transport, may be unaffordable if they were profitable; in such circumstances, the State has to supply consumers who could not use them otherwise due to their low income.[127] This is also the mechanism that the new Electricity Market Directive (EU) 2019/944 favours because it does not affect competition between suppliers.[128]

(124) A special element of affordability relates to the availability of an offer with only the minimum service that is required. Thus, under the heading of 'control of expenditure', Article 88 of the European Electronic Communications Code requires Member States to ensure that designated undertakings, in providing facilities and services additional to the minimum universal service, establish terms and conditions in such a way that the subscriber is not obliged to pay for facilities or services which are not necessary or not required for the service requested. Similarly, Article 16(9) of the Payment Accounts Directive requires Member States to ensure that access to a payment account with basic features is not made conditional on the purchase of additional services or of shares in the credit institution, unless the latter is conditional for all customers of the credit institution.

c) Non-discrimination and equality

(125) Another typical feature of SGI even beyond universal service obligations is the principle of non-discrimination or of equality. Discrimination on grounds such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or

---

124 For detailed discussion, see de Streel and Hocepied, n 117, 96.

125 See S. Pront-van Bommel, A Reasonable Price for Electricity, *Journal of Consumer Policy* 39 (2016), 141 ff.

126 ECJ, 6 October 2015, Case C-508/14 *T-Mobile Czech Republic and Vodafone Czech Republic*, ECLI:EU:C:2015:657.

127 See H.-W. Micklitz, The Politics of Justice in European Private Law: Social Justice, Access Justice, Societal Justice (Cambridge University Press, 2018), 299 ff,

128 See Article 5(2) of Directive (EU) 2019/944.

any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation is prohibited under Article 21 of the Charter of Fundamental Rights, and as mentioned above, the Court of Justice has held that prohibition of discrimination has horizontal effect between private parties.

(126) Provisions prohibiting discrimination can also be found in EU secondary law on SGI. According to Article 15 of the Payment Accounts Directive 2014/92/EU, Member States shall ensure that credit institutions do not discriminate against consumers legally resident in the Union by reason of their nationality or place of residence or by reason of any other ground as referred to in Article 21 of the Charter, when those consumers apply for or access a payment account within the Union. The conditions applicable to holding a payment account with basic features shall be in no way discriminatory.

(127) Similarly, Article 99 of the European Electronic Communications Code prohibits providers of electronic communications networks or services to apply any different requirements or general conditions of access to, or use of, networks or services to end-users, for reasons related to the end-user's nationality, place of residence or place of establishment, unless such different treatment is objectively justified. According to Article 5(1) of the Postal Services Directive 97/67/EC, universal service shall be provided without any form of discrimination whatsoever, especially without discrimination arising from political, religious or ideological considerations.

(128) Going beyond the prohibition of discrimination, EU secondary law enshrines the principle of equality specifically for universal service obligations. For example, the basic service under the Telecommunications Universal Service Directive 2002/22/EC was to be made available at a base tariff that should be equal to all consumers of a specific area, and Article 85(2) of its successor, the European Electronic Communications Code, allows Member States to require universal service providers to apply common tariffs, including geographic averaging, throughout the territory. Article 5(1) of the Postal Services Directive states that universal service means identical service to users under comparable conditions.

d) Quality

(129) According to the European Commission, a high quality of SGI must be ensured. Where there is effective competition, high quality should not be an issue.

(130) The high quality criterion by no means implies that all consumers within the EU will find the same conditions, nor will all services be available to everybody. What high quality means may also change over time, with new technologies becoming widely available. For example, the universal service requirement of Directive 2002/22/EC was limited to a single narrowband network connection, the provision of which could be restricted by Member States to the end-user's primary location/residence, and did not extend to the Integrated Services Digital Network (ISDN). Nevertheless, even the basic

service that every consumer had to have access to should have been of high quality. Thereby, defining the minimum quality standards to be kept is not a matter of contract law but of regulation;[129] whereas higher standards can of course be agreed by contract.

(131) The Payment Accounts Directive 2014/92/EU defines in Article 17 the basic features that a basic banking account must have.

(132) Quality requirements are also relevant in contract law. They come into play when service providers do not keep the quality standard that was promised or that is required by law, and that the consumer pays for. Article 10(3) lit. f) of the Electricity Market Directive (EU) 2019/944 demonstrates that the EU takes liability for failing to meet quality requirements as a given when it requires the service provider to inform on the respective compensation and refund arrangements.[130]

e) Continuity

(133) According to the Commission, continuity means that the provider of the service is obliged to ensure that the service is provided without interruption.[131] One example is Article 3(1) of the Postal Market Directive 97/67/EC, which obliges Member States to 'ensure the permanent provision of a postal service'. Postal services shall not be interrupted or stopped except in cases of *force majeure*.[132] Article 108 of the European Electronic Communications Code provides such a continuity requirement generally in relation to all end-users.

(134) In terms of the contractual relationship between the consumer and the supplier, for example of electricity or telecommunications services, the supplier may be in breach of contract if the service breaks down temporarily; and he may be liable for damages the consumer suffers.

5. Protection of vulnerable consumers

(135) A more recent element of the law on SGI is the special recognition of the needs of so-called vulnerable consumers.[133] This is most prominent in electricity law where the Electricity Market Directive (EU) 2019/944 dedicates two provisions – Articles 28 and 29 – to vulnerable customers and energy poverty, but we also find certain elements of it in telecommunications law and in the Payment Accounts Directive 2014/92/EU. In

---

129 The White Paper on Services of General Interest, n 104, 5.

130 See Green Paper on Services of General Interest, n 118, 48.

131 ibid., 17.

132 Article 5(1) of Directive 97/67/EC.

133 For the development of this area, see P. Rott, Liberalisation and protection of vulnerable customers in SGI, *Europarättslig Tidskrift* 2011, 483 ff.

these areas, vulnerability mostly relates to low-income or other deplorable circumstances, such as being homeless. For example, although prices shall be non-discriminatory, social tariffs have been permitted to support vulnerable consumers.[134] According to Article 85(2) of the European Electronic Communications Code, where Member States establish that, in light of national conditions, retail prices for the services referred to in Article 84(1) are not affordable, because consumers with a low income or special social needs are prevented from accessing such services, they shall take measures to ensure affordability for such consumers of adequate broadband internet access service and voice communications services at least at a fixed location.

(136) In relation to payment methods, Article 10(7) of the Electricity Market Directive (EU) 2019/944 states that household customers who have access to prepayment systems – and these are typically on low income - shall not be placed at a disadvantage by the prepayment systems.[135]

(137) The Electricity Market Directive (EU) 2019/944 also mentions geographic vulnerability. Member States shall take measures to protect customers in remote areas; although this should rather be characterized as an equality issue.

(138) Vulnerability due to disability is addressed by Article 111 of the European Electronic Communications Code. The provision requires Member States to ensure that the competent authorities specify requirements to be met by providers of publicly available electronic communications services to ensure that end-users with disabilities: a) have access to electronic communications services, including the related contractual information provided pursuant to Article 102, equivalent to that enjoyed by the majority of end-users; and b) benefit from the choice of undertakings and services available to the majority of end-users. Moreover, Article 85(4) of the European Electronic Communications Code provides for state support and potentially other measures to ensure that terminal equipment, and specific services that enhance equivalent access, including where necessary total conversation services and relay services, are available and affordable.

(139) As no consumer wants to access electronic communications services without a reason, this implies that the consumer only benefits from this provision if she can also use these services, and in particular the ones mentioned in Article 84(3) with Annex V, despite her disability.

---

134 In the new Electricity Market Directive, however, the EU legislator clearly wants to phase out social tariffs and replace them by direct support by welfare authorities; see Article 5(2) of Directive (EU) 2019/944.

135 Higher prices due to the use of prepaid meters have been common practice in the past.

V. Applying the SGI Model to Digital Platform Services

1. Introduction

(140) The European Commission's consultation on the Digital Services Act is indicative of a desire at EU level to take further action to regulate the power and activities of certain digital service providers. In this section, we shall consider whether the SGI model outlined above would act as a suitable framework for such regulation.

(141) In particular, we will first (section 2) identify the problems that categorising digital platforms as SGI would seek to address. As Bennett-Moses suggests, a necessary starting point for regulation is to identify a societal harm or problem that needs to be addressed, rather than an addressee of regulation.[136] In a similar vein, Sauter emphasises that while SGI is a dynamic concept that varies 'between time and place'[137] and should not be defined, it is strongly linked to market failure. He therefore proposes that consumer rights that are inadequately provided for by the market be identified to guide the imposition of SGI obligations.[138] Therefore, in sections (3) and (4) we identify relevant market based and universal service obligations (respectively) that could be applied to digital service providers. Finally, we consider (5) who the addressees of such SGI obligations might be.

2. Digital service platforms as essential services

(142) Historically, the task of identifying what constitutes a SGI and therefore who should be subject to additional regulatory obligations is a competence left to EU Member States. This task was left to Member States because the provision of SGI was typically funded nationally and therefore required solidarity between those funding their provision and the wider beneficiaries. Moreover, this respected the sovereignty of Member States when organising their public services and was an acknowledgement of the different cultural, political and social positions of the Member States as well as the differences in their administrative organisation.

(143) Consequently, much of the doctrine categorising and defining SGI has focused on identifying common criteria across Member States in the classification of a service as an SGI. The primary input of the Commission to date in this process has been through its oversight role. As the designation of a service as an SGI led to the more limited

---

136 L. Bennett-Moses, 'How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target', 5(1) *Law, Innovation and Technology* (2013), 1, 17.

137 W. Sauter, 'Services of general economic interest and universal service in EU law', *European Law Review* 2008, 167

138 Ibid, 189.

application of certain Treaty provisions, in its capacity as guardian of the Treaties the Commission could assess whether Member States had 'manifestly erred' in classifying a particular service as an SGI. The Commission has however supplemented this role by enacting sectoral legislation in liberalised network industries, such as telecommunications, postal services and transport, imposing SGI obligations.

(144) The introduction of an explicit legal basis of the EU to legislate in the field of SGI by setting the principles and conditions which enable them to fulfil their mission paves the way for wider EU initiatives to facilitate SGI provision.[139] This provision - Article 14 TFEU - recognises that any such regulation must be 'without prejudice to the competence of Member States, in compliance with the Treaties, to provide, to commission and to fund such services'. No doubt mindful of subsidiarity considerations, the Commission has adopted a cautious approach to the designation of new sectors as SGI.[140] Nevertheless, the Commission has also explicitly stated that given that 'users' needs and technologies evolve constantly, it is necessary to review regularly both existing universal service obligations and the need to introduce new ones'.[141] We propose that the platform services sector is one such sector where intervention is now ripe on the basis of both technological evolution and changes to users' needs.

a) Recognition of digital services as essential services in existing EU legislation

(145) Digital platform services have not yet been directly recognised as SGI. Although 'functional internet access' forms part of the universal service obligations of telecommunication services providers under Directive 2002/22/EC, only a few EU Member States have made access to broadband internet a universal service that every citizen must be granted. The new Directive (EU) 2018/1972 establishing the European Electronic Communications Code will improve the situation in that it requires Member States to ensure that all consumers have access at an affordable price to an available adequate broadband internet access service.[142] The precise definition of 'adequate' in the context of Article 84(3) is left to the Member States. However, Annex V of the Directive sets out the minimum services which an adequate broadband internet access service should be capable of supporting. This list includes e-mail, search engines, basic training and education online tools, online newspapers or news, buying or ordering goods or services online, job searching and job searching tools, professional

139 A Quality Framework for Services of General Interest in Europe, n 106, 3 f.

140 ibid., 5.

141 ibid., 9.

142 OJ 2018, L 321/36. See Article 84(1) of Directive (EU) 2018/1972.

networking, internet banking, eGovernment service use, calls and video calls (standard quality) and social media and instant messaging.[143]

(146) Thus, access to services that some of the most powerful digital players provide, such as search engines (Google), buying or ordering goods (Amazon), social media (Facebook, Twitter), video calls (Skype), is therefore indirectly recognised to be of relevance for people's social and economic life. This is also confirmed by recital 213 of the Directive which recognises that adequate broadband internet access 'provides the basis for participation in the digital economy and society through essential online internet services'. We can therefore observe that while the obligations set out in this Directive relate only to internet access as such, many of the services themselves are equally essential to the social and economic lives of European residents.

(147) Further recognition of the significance of reliable access to digital content and services for EU residents is found in the Net Neutrality Regulation 2015/2120/EU,[144] part of the telecommunications package. This Regulation provides that:

> End-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service.[145]

(148) This Regulation recognises the competitive implications of unreasonable traffic management practices but also the fundamental rights implications of such discrimination between content. It explicitly notes that its provisions are designed to ensure respect for the fundamental rights set out in the EU Charter including freedom of expression and information, data protection and non-discrimination, amongst others.[146] That discrimination by Internet Service Providers raises significant human rights issues has been noted by the (non-EU) Council of Europe, responsible for human rights protection. It has noted that traffic management or preferential treatment by ISPs should not:

> diminish or affect the affordability, performance or quality of user's access to the Internet. Internets users must….be informed about the impact that such treatment might have on their ability to access, use and impart information, diverse and pluralistic content that is publicly available, applications and services of their choice.[147]

---

143 *See* Annex V of Directive (EU) 2018/1972.

144 Regulation (EU) 2015/2120 laying down measures concerning open internet access, OJ 2015 L 310/1. See also de Streel and Hocepied, n 117, 115 ff.

145 Article 3(1) of Regulation (EU) 2015/2120.

146 Recital (33) GDPR

147 Council of Europe, Recommendation on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality, CM/Rec(2016)1, 13 January 2015

(149) This Regulation therefore recognises the importance of preserving the freedom of choice of Internet users as well as their fundamental rights and indicates that legislative intervention was required to preserve such choice and fundamental rights. The imposition of SGI obligations on certain digital services would equally preserve choice and user rights at the content and applications layer of the digital ecosystem.

b) The essential roles of digital platforms

(150) The economic dimension of digital platforms is evident; the top five most valuable global brands in 2020 according to Forbes were all technology firms, famous for their digital platforms.[148] It is perhaps also unsurprising that digital service providers have been amongst the biggest beneficiaries of the current global pandemic, with Netflix, Amazon, Microsoft and Paypal all recording significant increases in value in 2020. However, beyond the economic, there are important reasons to classify the services offered by digital platforms as SGI.

(151) First, social interaction is one of the three planks of the pyramid of our essential needs, ranking alongside security and physiological needs.[149] Our social interaction increasingly takes place on digital platforms, ranging from social networking services to consumer communications applications. This is a trend that has been accelerated by the pandemic. Empirical evidence suggests that while many households have been confined to their homes in 2020, the average amount of time spent online has increased.[150] More of our social interaction needs are now necessarily fulfilled digitally.

(152) Second, beyond the purely social, we are also increasingly dependent on digital platforms for the provision of public and community services with a failure or inability to sign up to these platforms leading to de facto exclusion from essential activities and information. The WHO has, for instance, partnered with Facebook and WhatsApp to provide Covid-19 information updates to interested individuals.[151] While this approach has the advantage of reaching an audience of up to 2 billion users quickly and effectively, it also acts to draw users to the Facebook family of products and services where they might otherwise have opted for an alternative service. Similarly, whereas an individual might have a choice as to whether they use Google Search to conduct search queries online, if a child attends a school that opts to conduct remote learning

---

148 There were: Apple, Google, Microsoft, Amazon and Facebook. For the methodology and full-list see, https://www.forbes.com/the-worlds-most-valuable-brands/#2f7201c6119c.

149 For the first mention, see A. Maslow, 'A Theory of Human Motivation', 50 *Psychological Review* (1943), 370 ff.

150 In the UK, internet users were spending on average 3 hours 24 minutes online daily with the majority of this spent using a relatively narrow set of sites however in April 2020 this increased by 32 minutes daily. The CMA Report, n 11, 47.

151 African News Agency, 'Covid-19: WHO health alert brings facts to billions via WhatsApp', *Independent Online*, 21 March 2020.

via the Google Classroom learning technology this child has no choice but to engage with the Google ecosystem.[152] Such public-private partnerships are likely to increase in the coming years, making some digital service platforms de facto essential and putting the conditions under which users are granted access to these platforms under increasing scrutiny.

(153) Third, by intermediating the majority of our digital interactions, digital service providers are in a privileged position to determine the extent to which we can exercise our fundamental rights.[153] For instance, our freedom of expression and information can be impacted by content moderation policies that amplify the visibility of certain content while rendering other content invisible to us. The effectiveness of our data protection and privacy are also affected by the data processing policies of digital platform providers. Excessive data processing practices legitimised by consent and broadly stated purposes of processing, or cross-platform data sharing that does not respect the initial context in which the personal data were processed, render the idea of informational self-determination redundant.

(154) Finally, and on a related note, digital service platforms exercise a quasi-regulatory function themselves. The way in which technological design (or code) can act as a modality of regulation of individual conduct has been observed since *Lessig* famously declared in 1999 that 'Code is Law'.[154] However, in addition to design choices, digital service providers govern the interactions between users, and users and third parties through their terms of service, amongst others.[155] While again such private governance is not new, the number of individuals subject to such private governance by digital service platforms exceed those of nation states and supranational entities like the EU. Platforms should therefore be recognised as institutions with a 'regulatory function' and their governance mechanisms overseen as such.[156] Indeed, in a note relating to the proposed Digital Services Act, the European Commission stated in the context of oversight of illegal speech that 'many public interest decisions that should be taken by independent public authorities are now delegated to online platforms, making them

---

152 DefendDigitalMe, Google Education Products under Scrutiny: lawsuit in New Mexico and Norway DPA investigates, February 2020.

153 E.B. Laidlaw, Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility, (Cambridge University Press, Cambridge, 2015); O. Lynskey, 'Regulating "Platform Power"', LSE Legal Studies Working Paper No. 1/2017 (2017).

154 L. Lessig, Code and Other Laws of Cyberspace Ver. 2.0 (Basic Books, 2006).

155 L. Belli and J. Venturini, 'Private ordering and the rise of terms of service as cyber-regulation', *Internet Policy Review* 5(4) (2016).

156 The Special Advisors' Report, n 19, 60-63.

de-facto regulators without adequate and necessary oversight, even in areas where fundamental rights are at stake.'[157]

3. *Relevant market-related obligations*

a) Promoting a competitive market through access to data

(155) As suggested above, access to data may be essential to compete in some digital markets. For instance, it is arguable that Google search engine is shielded from effective competition on the market for internet search on the basis that it has accumulated a vast dataset of search queries and reactions to search queries. This dataset can then be used to train its algorithm in order to further refine the search results that it offers to users. Providing actual and potential competitors with access to all or part of this dataset (for instance, anonymised search queries) on fair, reasonable and non-discriminatory (FRAND) terms might therefore enhance competition in this market.

(156) This would however require a market specific assessment. Relevant factors to consider would be whether it is data, the algorithm used to generate search results, or other factors that are decisive to compete on the market. Moreover, given the difficulty in anonymising datasets effectively, the GDPR is likely to impose a regulatory constraint on data sharing making the mass transfer of datasets cumbersome and likely undesirable.

b) Promoting choice through access to infrastructure

(157) Providing access to the underlying infrastructure, as opposed to the data processed through this infrastructure, is another possibility to facilitate choice on digital platform markets. This can be done through an interoperability mandate, a proposal that is gaining increasing support in the digital platforms context.[158] The primary advantage of this approach is that it could break the lock-in effect users currently experience on many digital platforms. For instance, users concerned about Facebook's exploitation of personal data for political micro-targeting and other forms of aggressive advertising might be reluctant to leave the platform due to the loss of connectivity with contacts this would entail. Interoperability would enable the user to maintain the advantage of Facebook's network effects – a wide pool of contacts – while simultaneously using a platform or application that more closely aligns to their needs and interests. Or, as

---

157 https://cdn.netzpolitik.org/wp-upload/2019/07/Digital-Services-Act-note-DG-Connect-June-2019.pdf, 3.

158 P. Marsden and R. Podzsun, 'Restoring Balance to Digital Competition – Sensible Rules, Effective Enforcement (KAS, 2020); L. Zingales and F.M. Lancieri, 'Stigler Committee on Digital Platforms: Policy Brief', *Stigler Center for the Study of the Economy and the State* 2019.

Doctorow puts it, interoperability 'presents a means for people to remain partially on Facebook, but while using third-party tools that are designed to respond to their idiosyncratic needs'.[159] In this way, Facebook users could gradually siphon off the platform into other communities. While interoperability is most frequently discussed in the context of social networking and consumer communications applications (where an easier analogy can be made to telecommunications interoperability), interoperability is also deployed in other sectors to other ends beyond communications. A good example is 'Open Banking' where banks were asked to create new open Application Programming Interface (API) standards to enable third parties to access consumer bank accounts and to offer a range of new services to consumers (such as lower transaction fees for bank transfers).[160]

(158) It is difficult to find agreement on a definition of interoperability, perhaps because there are several ways in which interoperability has been categorised. Article 2(12) of Directive (EU) 2019/770 on contracts for digital content and services[161] defines interoperability as 'the ability of the digital content or digital service to function with hardware or software different from those with which digital content or digital services of the same type are normally used'. Some categorise data sharing agreements as a light form of interoperability. For instance, the Special Advisors' report considers 'data interoperability' to be like data portability but 'with real-time, potentially standardised, access for both the data subject/machine user and entities acting on his or her behalf'. Some such existing mechanisms do exist; they give the example of access tokens, which a user can give to a service provider (A) to access the user's data on service (B) through service B's API. Through this example, we can see that data interoperability requires some level of protocol interoperability.[162]

(159) When 'interoperability' is referred to in this context, it is generally protocol interoperability that is discussed. This enables two systems to work together fully. It enables the provision of complementary services; within platforms (where services connect to a host platform) or between services (for instance, where a range of devices connected or interoperate with one another in the Internet of Things context). Full protocol interoperability enables substitute systems to interoperate. It therefore

159 C. Doctorow, 'Interoperability and Privacy: Squaring the Circle', *Electronic Frontier Foundation,* 13 August 2019, available at: https://www.eff.org/deeplinks/2019/08/interoperability-and-privacy-squaring-circle [Accessed on 4 October 2010).

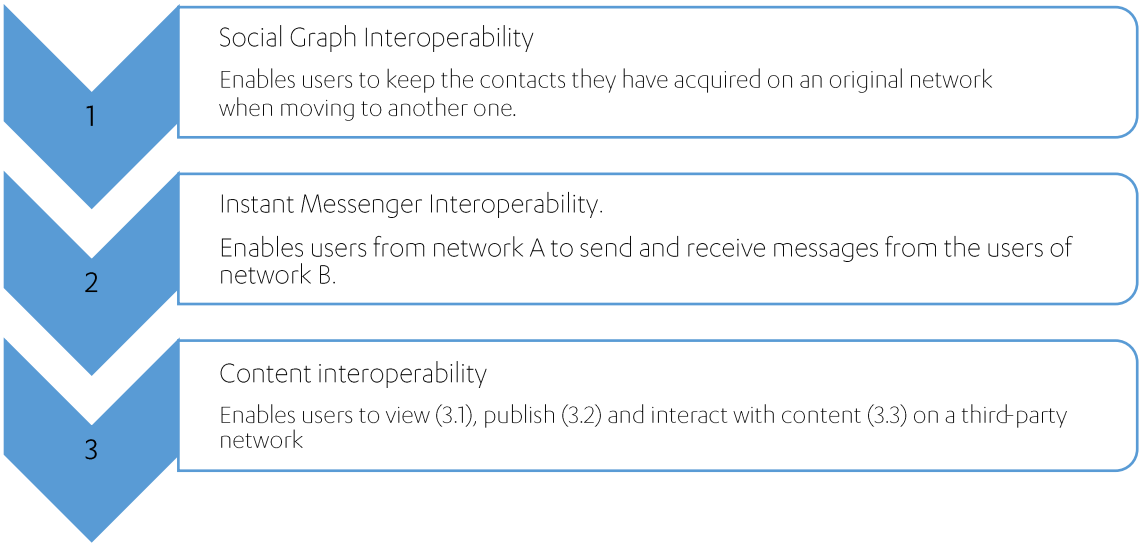
160 Organisation for Economic Co-operation and Development, Working Party No. 2 on Competition and Regulation, 'Line of Business Restrictions - Background note by the Secretariat', DAF/COMP/WP2(2020)1, 19 May 2020, para 109.

161 OJ 2019 L 136/1.

162 Doctorow, n 159, distinguishes between data portability; back-end interoperability and delegability.

requires further integration and consensus around a common standard. Common examples include e-mail and mobile phone networks.

(160) The French *Conseil National du Numerique* advises against full protocol interoperability based on the evidence it gathered. Instead, it proposes a system of graduated non-exclusive options of interoperability for social networking services based on the functionality concerned. This would proceed as follows:



(161) This kind of tiered interoperability may be appropriate for platform services where full protocol interoperability is deemed unnecessary. Indeed, some level of interoperability is already foreseen for 'number-independent interpersonal communications services' in the new Directive establishing a European Electronic Communications Code (EECC). These services are defined as those which do not connect with publicly assigned numbering resources (such as a fixed line phone number).[163] In this context, this would include services such as consumer communications services like Skype, Zoom and Whatsapp. In particular, Article 61(2)(c) specifies that a competent authority may impose obligations on relevant providers to make their services interoperable where end-to-end connectivity between end-users is endangered as a result of a lack of such interoperability and such interoperability is necessary.[164]

(162) What is notable about the French report, and supported here, is that interoperability is not conceived of as a tool for pure competition purposes. Rather, it is recognised as

163 Article 4(7) of the European Electronic Communications Code.

164 See further, de Streel and Hocepied, n 117, 75 f.

a consumer right, in so far as it responds to the needs of consumers to gain control over their data and to have their digital tools to interact.[165]

(163) How then can interoperability be delivered? As discussed below (addressees of SGI obligations), a first step is to identify the markets in which such intervention is required to restore consumer sovereignty and address the digital asymmetry. Once identified, it is necessary to determine which form of interoperability is required and to create minimum standards for interoperability.[166] This standardisation process 'would set a 'floor' for how interoperable very large platforms must be'.[167] *Marsden and Nicholls* outline how this might operate where regulation sets out an interoperability mandate.[168] They differentiate between access providers and access seekers (as in telecommunications regulation). Where an access seeker requests access to the API of an access provider, the access provider must, at a minimum, provide access to the API and take reasonable steps to ensure that the technical and operational quality of the API is equivalent to that available to the access provider.[169] In terms of pricing, as noted, providing access to the API could be based on Fair, Reasonable and Non-Discriminatory (FRAND) terms. Non-price access terms and conditions would also need to be set out in advance.

(164) The need for this type of interoperability is likely to increase as datafication proceeds at pace and new digital bottlenecks emerge.[170] For instance, *Brown* notes that the BBC's Director of Radio stated in a parliamentary hearing that the BBC had been unable to agree deals with Amazon and Google for smart speakers to carry BBC coronavirus coverage.[171] Enabling the users of these digital assistants to assume more control over

---

165 Le Conseil National du Numerique (CNN), Concurrence et regulation des plateformes: Etude de cas sur l'interoperabilite des reseaux sociaux, 2020.

166 B. Cyphers and C. Doctorow, 'A Legislative Path to an Interoperable Internet', Electronic Frontier Foundation, 28 July 2020, available at https://www.eff.org/deeplinks/2020/07/legislative-path-interoperable-internet#:~:text=Interoperability%20is%20corporate%20entropy.&text=This%20would%20set%20a%20%E2%80%9Cfloor,gates%20and%20let%20others%20in [Accessed on 4 October 2020]; C. Mardsen and R. Nicholls, 'Interoperability: A Solution to regulating AI and social media platforms', SCL - Tech Law for Everyone 2019, available at https://www.scl.org/articles/10662-interoperability-a-solution-to-regulating-ai-and-social-media-platforms [Accessed on 4 October 2020].

167 Cyphers and Doctorow, n 166.

168 Mardsen and Nicholls, n 166.

169 They differentiate between situates where the access operator has an API and those where the access operator creates an API, suggesting distinct obligations in the two scenarios. The first category can encompass the second and therefore this distinction is not essential.

170 The EFF also recommends that a general legal right to interoperate be provided for by law. This 'adversarial interoperability' would place a prohibition on platform providers from preventing the development of interoperable segments on its platform. The EFF makes the valid point that in telecommunications you do not need the phone company's authorisation to design a device that works with its system.

171 I. Brown, 'Interoperability as a tool for competition regulation', 2020, preprint available at: https://osf.io/preprints/lawarxiv/fbvxd.

what content they receive and how the service is configured will be key to addressing ongoing digital asymmetry.

(165) There are nevertheless distinguished voices who consider that the extension of full protocol interoperability from physical infrastructures (such as telecommunications) to digital platforms is not an obvious choice. *Kerber and Schweitzer* seek to distinguish these two applications on the basis that neither 'the goal to prevent market tipping nor the universal service rationale are relevant across the board when it comes to digital platforms'. [172]

(166) Their concern with regard to tipping is that, even where it may be a concern, the 'imposition of interoperability duties upon a digital platform may imply a significantly more interventionist regime than the interconnection requirement between physical networks'. Presumably this is deemed more interventionist as API access mandates shape the way in which a product is designed, and the decision to, for instance, operate a walled garden.[173] This is a valid point and such design choices are often driven by concerns to maintain standards in areas such as security. Nevertheless, it is this very design choice which has far-reaching consequences for consumers and society more broadly, and it is therefore necessary to recognise that maintaining the status quo is not without significant consequence.

(167) Their second concern is that universal service policies should simply strive to ensure a basic service (as opposed to end-to-end connectivity). This concern is premised on the idea that consumer sovereignty over the terms on which personal data are processed and the policies based on which digital content is moderated and presented to platform users is peripheral to the core service offered to users. Nevertheless, these features are central to the service offered – part of the 'basic service' – just as the ability of an Internet user to access the content of their choice without unreasonable discrimination is central to the provision of Internet access and protected by net neutrality regulation. The claim that multi-homing will mitigate this issue is perhaps over-stated. As the CMA notes in the context of social networking sites:

> 'consumers' use of multiple [social media] platforms does not necessarily imply that their services can be used as substitutes by consumers and that these other platforms can meet the same consumer needs as Facebook.'

(168) It notes that while users of other platforms cross-visit Facebook, a much lower proportion of Facebook users cross-visit other platforms. This indicates that Facebook

---

172 W. Kerber and H. Schweitzer, 'Interoperability in the digital economy', *Marburg Centre for Institutional Economy, Macie Paper Series* No. 2017/02, 1, 18.

173 P. Ibanez Colomo, 'Apple's App Store: a microcosm capturing what digital cases are all about', *Chillin' Competition*, 21 August 2020, available at: https://chillingcompetition.com/2020/08/21/apples-app-store-a-microcosm-capturing-what-digital-cases-are-all-about [Accessed on 4 October 2020].

is a 'must-have platform'; the use of other platforms is nearly always in combination with Facebook.[174]

(169) In order for interoperability of digital platforms to succeed in this context, a number of other potential pitfalls need to be borne in mind and avoided. First, the standardisation process should not lead to market paralysis. For instance, the founder of Signal messaging service has noted that in a federated ecosystem (with open APIs), it becomes very difficult to make changes. He suggests this is the reason why e-mail does not have end-to-end encryption while an unfederated service such as WhatsApp was able to 'introduce end-to-end encryption to over a billion users with a single software update'.[175] Further reflection is needed on how a balance can be struck between preventing dominant companies from leveraging their power in the standardisation process excessively, and ensuring the process does not stagnate in a way that is harmful to competition and consumer sovereignty. The EFF suggests for instance that standardisation does not need to take place by Committee but rather ex post oversight of the terms on which the API access is offered to ensure they are FRAND should be sufficient.[176]

(170) Another pitfall to avoid relates to critical policies offered to platform users on issues such as data protection and content moderation. From a data protection and privacy perspective, one concern is whose data protection policy (and data processing practices) would prevail in an interoperability scenario. If, for instance, a user of a new social networking site contacted a Facebook user facilitated by an interoperable API, one may query whether the meta-data about the communication would be available for both social networking sites to process and what data protection policy would apply to such processing. If it were the policy of the hosting servers (here Facebook) then this may do little to alleviate the concerns of those who are using other platforms to avoid Facebook for privacy reasons. One preliminary observation is that the mere fact of introducing interoperability would not in any way reduce the need for robust data protection enforcement. Civil liberties organisations, EDRi and the EFF both suggest that the data processing in the scenario above should be limited to that which is strictly necessary to support interoperability and that there should be no monetisation of such data.[177] Such constraints would need to be clearly identified in advance and respect EU data protection law.[178] Indeed, the constraints 'read into' the right to data portability

---

174 The CMA Report, n 11, 129.

175 M. Marlinspike, 'Reflections: The ecosystem is moving', *Signal Blog* 10 May 2016, available at: https://signal.org/blog/the-ecosystem-is-moving [Accessed on 4 October 2020].

176 Cyphers and Doctorow, n 166.

177 I. Brown, n 171, at 23.

178 This is reiterated by the CNN, n 165, 9.

by the Article 29 Working Party go beyond those explicitly mentioned in Article 20 GDPR; the same could be done here.[179]

(171) The same logic would apply to content moderation policies. This is an aspect of interoperability and federation where more research is needed, as *Brown* notes.[180] The EFF considers that as long as decisions regarding interoperable communications are user-initiated and well-informed concerns regarding control over data and content spamming can be addressed. It notes that users are currently able to cross-post content from Instagram to other platforms (including Facebook but also Twitter and Tumblr) which suggests that Facebook could design its functionality in a way that protects against those concerns.

c) Information for oversight purposes

(172) Independent third-party auditing is not mandated by the GDPR but rather is listed amongst the potential 'good practices' for controllers when deploying solely automated decision-making.[181] Ongoing oversight of algorithmic operations is not therefore required by the GDPR and is one additional systemic transparency measure that should be considered. *Cobbe and Singh* suggest, as a starting point, that algorithmic recommendation systems should be mandated to 'keep logs of recommended content (both for personalisation and for behavioural targeting) so that they can be reviewed by users and by oversight bodies'.[182] This is by no means the only way in which such systemic transparency could be facilitated.

(173) Indeed, one could envisage comparison websites, as required for 'classical' SGIs, that could, for example, compare the requirements concerning the permission for the platform operator to use and share the consumers' personal data as well as the consumer's right to avoid that permission by payment in money (see also infra, 4. b).

---

179 The Article 29 WP, 'Guidelines on data portability' (WP242rev.01), adopted on 5 April 2017, 12 which states that: 'to prevent adverse effects on the third parties involved, the processing of such personal data by another controller is allowed only to the extent that the data are kept under the sole control of the requesting user and is only managed for purely personal or household needs. A receiving 'new' data controller (to whom the data can be transmitted at the request of the user) may not use the transmitted third party data for his own purposes e.g. to propose marketing products and services to those other third party data subjects…'.

180 *Brown,* n 171, 27, notes that further research is needed on 'how federation might encourage hate-speech online and ways to manage those groups', as well as 'the extent to which topology, abstraction, and scale facilitate problematic online behavior'.

181 EDPB, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.0), adopted on 6 February 2018, 32.

182 J. Cobbe and J. Singh, 'Regulating Recommending: Motivations, Considerations and Principles', *European Journal of Law and Technology* 2019 (online access), 17.

4. Relevant Universal Service Obligations

a) Access

(174) In terms of access, we can refer to the usual universal service approach. Access means, first of all, that platforms should have to accept all interested consumers. That does not mean that specialized platforms for only particular types of users or services should not be allowed; however, where services are offered to the general public, an obligation to contract should be in place. Denial of access must therefore limited to overarching reasons, such as previous consistent breach of the platform contract.

(175) In the same way, termination of the platform contract must be limited to such overarching reasons; similar to what applies to payment accounts with basic features, and procedures must be in place by which the consumer can complain against such termination, ideally before it takes place. Also, termination of the contract should be preceded by less stringent measures, such as a warning – as we know it from electricity supply – or a temporary suspension of the service.

b) Affordability

(176) Digital content and services are often made available to individuals without a monetary cost. As such, the financial affordability of such content and services is not in question. However, their availability is currently subsidised primarily through advertising revenue, in particular behavioural advertising that necessitates the monetisation of personal data. Personal data has therefore been recognised in EU law as the 'price' paid by consumers for such access, for example in the new Article 3(1a) Consumer Rights Directive, as amended by the Omnibus Directive, and in recital (16) of the European Electronic Communications Code.

(177) This begs the question of whether the quantity or the nature of the personal data extracted is excessive in relation to the service or content provided thus rendering them 'unaffordable' from a data protection perspective. There are several avenues through which such an assessment could be made in the GDPR, discussed above. Competition law also affords an opportunity to assess this contractual exchange where the digital service provider is dominant. As the CMA report notes, while consumers do not pay a monetary price for platform access, it is possible that in a more competitive market consumers might not need to provide so much data in exchange for such access or that the price would be a negative one, where they are rewarded for platform use.[183] Therefore, just as the exploitative abuse of excessive pricing provides an opportunity to assess whether the price offered to customers goes beyond enabling a

183 CMA Report, n 11, 69 f.

dominant company to ensure a reasonable return on investment, so too could excessive data extraction enable such an assessment.[184]

(178) While excessive data extraction was at the core of the Facebook Germany case, it was not reasoned in this way. The German Federal Supreme Court in its preliminary decision concluded that Facebook was dominant in a market for social networking services in Germany and had abused this dominant position by extracting data from consumers when they were not using the Facebook platform (through 'off-Facebook' data collection). While the *Bundeskartellamt* had considered that Facebook abused its dominance by violating the GDPR consent requirement (thereby using data protection as a normative benchmark for an anti-competitive infringement), the German Federal Supreme Court reasoned otherwise. Its reasoning was anchored in the broader constitutional notion of informational self-determination, or individual control over personal data, which can be linked to consumer autonomy. The 'off-Facebook' data processing practices violated this principle.

(179) What is of interest for present purposes is the remedy endorsed by the *Bundesgerichtshof* (assuming that the preliminary decision is confirmed in the final judgment, which is highly likely). The court held that Facebook has to offer the consumer a true choice between subscribing to the service with and without their personal data on Facebook being connected with personal data that has been collected off Facebook. Such a remedy would give some control over cross-platform personal data leveraging. Indeed, access to digital content and services is often conditional on this type of data leveraging. The CMA notes, for instance, that Google and Microsoft both aggregate consent across their services with their privacy policies confirming that they use data processed across other parts of their business.[185]

(180) It prompts two preliminary queries. First, will such a measure truly empower users or will it place even more pressure on an already pressured consent mechanism? Second, this measure simply concerns off-Facebook data processing, could competition law be used to place limits - and to force such a choice - for 'on-Facebook' data processing?

(181) While ambitious interpretations of both competition law and data protection may lead us to such a 'choice requirement' for consumers, we have limited precedent for such a finding so far. This is a gap which the UK Competition and Markets Authority proposes to fill by giving a new Digital Markets Unit the power to impose a 'choice requirement' on platforms, whereby digital platforms would be required to provide consumers with the choice not to share their data for the purposes of personalised advertising.[186]

---

184 V.H.S.E. Robertson, 'Excessive data collection: Privacy considerations and abuse of dominance in the era of big data', 57 *Common Market Law Review* (2020), 161 ff.

185 The CMA Report, n 11, 192.

186 Ibid, 379.

Provision for a similar requirement in an ex ante EU instrument would facilitate consumer autonomy and alleviate some of the competitive concerns raised by such cross-platform leveraging of assets.

c) Continuity

(182) In relation to digital platforms, uninterrupted service is of course important as well. However, it would seem difficult to derive consequences from a breakdown, at least when it comes to communication services. Also, reduction in price as a contract law consequence is difficult to imagine where the price is the conferral of personal data and/or the acceptance of personalised advertising. This could be different though if suppliers were obliged to offer their services for money rather than personal data.

(183) More salient is probably the situation when the service is phased out entirely, which would put the consumer at risk to lose her digital social environment. Of course, a private entity cannot be forced to maintain a service that does not pay out. If it was recognised as a service of general interest, though, the State could be allowed to support the service to keep it alive, as States are allowed to support public transport. Anyway, there should be a possibility for other suppliers to take over, which, again, requires interoperability of platforms and portability of data, as discussed above.

d) Protection of vulnerable customers

(184) Given the fact that EU secondary law calls for the protection of vulnerable customers in telecommunication services that are mediated by platforms, it seems indispensable that the platform themselves, acting as gatekeepers, have the same obligations. The communication needs of isolated elderly persons in times of COVID-19 shall suffice for illustration.

5. Addressees of SGI Obligations

(185) As suggested above, in principle the case for extending sectoral obligations to digital platforms as SGI can be made on the basis of the prior recognition of many of the services they offer as indispensable for Internet users; the important social role played by digital platforms; their impact on the effectiveness of fundamental rights in the digital sphere; and, the regulatory role that digital platforms play. Nevertheless, we should also recognise that digital platforms are not a homogenous group and not all digital platforms play this critical role for internet users. This raises the question: on the basis of what criteria should we determine whether a digital service should be deemed ‘essential’, and should this designation apply to all such digital services or only a subset of the overall category?

a) The designation of a service as essential

(186) The absence of criteria for the designation of a service as 'essential' means that the concept of SGI is a dynamic and flexible one. Adopting a needs-oriented perspective, we might start by asking what is required to participate meaningfully in daily life. We suggest that the essentials of daily life include participation in the following: social interaction; political engagement; publicly funded services, including education; community organisations; personal finances and the labour market. This is reflected to some extent in the list of services set out in Annex V of the EECC that adequate broadband access should facilitate (including job searching tools, internet banking, eGovernment service use, social media and search engines).[187]

(187) Not all digital services will be essential for participation in these various important facets of life. An SGI regulatory framework could therefore focus on those services which offer the only meaningful method of participation for users, or those where there are no viable (offline) alternatives available. This would require an initial assessment of what is currently deemed essential and ongoing review of the situation. As discussed above, while access to adequate broadband internet or basic banking was not considered such a necessity just over a decade ago, it is now.

b) A one-size-fits-all, or asymmetric obligation?

(188) Once a digital service is deemed essential (for instance, a social networking service or an eGovernment portal), the next question that must be addressed is whether the market-related and universal service obligations mentioned above apply to all providers of such services or a subset of these service providers.

(189) For the universal service obligations, it may be appropriate to extend the SGI regulatory obligations to all relevant market actors. In other sectors, EU secondary law on SGI usually leaves it to the Member States to determine which suppliers are obliged to provide universal services. For instance, according to Article 27(1) of the Electricity Market Directive, Member States may appoint a supplier of last resort, which they can do by appointing a specific supplier or by establishing general criteria. Thus, under German electricity law, the supplier of last resort is the supplier who has most customers in a given area. Member States can, however, also impose universal service obligations on all suppliers, or on all suppliers that fulfil certain criteria.

(190) Similarly, for the market-related requirements, it is appropriate to start from the position that such requirements can be extended to all market actors. The application of an interoperability requirement to all market actors might be necessary, for instance, where no single market player had a position of market power in a given

187 See Annex V of Directive (EU) 2018/1972.

market. However, in other contexts, it may be preferable to impose asymmetric obligations. One starting point for asymmetric obligations could be to use the market definition and dominance tools found in competition law. However, this is unlikely to be desirable for two reasons.

(191) First, as outlined briefly above, the exercise of market definition has come under increasing strain when applied to digital markets. As a result, we have seen various competition policy reports and reviews, as well as legislative initiatives, suggesting alternatives. In the UK, for instance, the Furman Report suggests that new obligations should be applied to firms with strategic market status. In identifying which firms have strategic market status it suggests that the aspects of market power particularly relevant to platforms and their potential to act as a bottleneck should also be considered for incorporation: economic dependence, relative market power and access to markets'.[188] Similarly, the 10th revision to the German Act against Restraints of Competition refers to entities that are of 'paramount cross-market importance for competition'. In assessing whether an entity is of such paramount cross-market importance for competition, the draft law identifies a number of relevant factors including, but not limited to, the possession of a dominant position on relevant markets. These include:

- Its financial strength or access to other resources;
- Its vertical integration and its activities in other related markets;
- Its access to data relevant to competition;
- The importance of its activities for third party access to markets and its associated influence on business activities.

(192) These proposals therefore move beyond the assessment of market power on a defined market as a starting point for regulatory obligations.[189]

(193) This is also recognised in the academic literature. *Van Dijk* likens platform environments to trees; with infrastructure representing the roots of the tree; intermediary platforms its trunk and its branches and leaves the wide array of applications and sectoral platforms.[190] As *Van Dijk* notes, by operating across these various layers, platforms gain more operative power. She attributes concentrations of power in the digital environment to at least three types of platformization dynamics: the vertical integration of platforms; the infrastructuralisation of intermediary

188 Digital Competition Expert Panel, 'Unlocking digital competition', March 2019, section 2.117.

189 This was a point already made by the Conseil National du Numerique in 2014 when it encouraged consideration of factors other than market share in assessing power in digital markets such as the power to 'undermine innovation through control of key resources, critical access points, visibility, information'.

190 J. Van Dijk, 'Seeing the forest for the trees: Visualizing platformization and its governance', *New Media & Society* 2020, 9.

platforms (where a platform acquires the status of infrastructure by virtue of its dense occupation of the intermediary layer)[191] and the cross-sectorisation of platforms (the way in which platforms operate across sectors enabling them to process data from multiple sectors). The authors of the CERRE Report on the DMA similarly suggest that while the DMA should cover all digital platforms particular obligations should be imposed on platforms that:

- Are large (this could be assessed based on the number of unique users; the time on the site etc)
- Hold an enduring gatekeeper position
- Orchestrate a digital ecosystem.

(194) This designation would be a time limited one.[192] This type of approach could therefore be used to identify entities to whom particular market-access obligations apply.

(195) In identifying the relevant criteria in this context, we can take into account those deemed relevant in the various competition law interventions above, however we can also rely on broader criteria given that the objectives of the imposition of SGI obligation are primarily to ensure that the provision of certain services is guaranteed to users to meet both economic and non-economic needs. Suitable criteria here might therefore include:

- The extent of vertical integration;
- The cross-sectorisation of the platforms present;
- Economic dependence on the relevant platforms;
- Societal/consumer dependence on the relevant platforms;
- The data processing practices of the platforms;
- The potential for cross-platform envelopment.[193]

(196) By developing criteria in order to guide when intervention is desirable that acknowledge not only the economic power of platforms but also their role in the social sphere as essential channels of interaction between individuals themselves and also between individuals, the private sector and, increasingly, the State, targeted SGI obligations could be imposed.

---

191 Van Dijk, ibid., notes that 'Mark Zuckerberg has often called Facebook a "social" infrastructure; with over two billion users, the social network has become a vital obligatory passage point for data flows passing through the trunk. Through its "family of apps" (WhatsApp, Instagram, Messenger, Login, Advertising, Analytics), Facebook is garnering a central position in the middle where it can connect content and data flows in the invisible backend.'

192 CERRE Report, n 97, 11.

193 This is defined as the way in which a firm can leverage its market power, user based and resources in one market (an origin market) into a new market (the target market). As Padilla highlights, not only can this lead to the potential monopolisation of the target market to the exclusion of as efficient competitors but it is also a credible strategy for a dominant firm to consolidate its market position on the origin market, see D. Condorelli and J. Padilla, 'Harnessing Platform Envelopment in the Digital World', *Journal of Competition Law and Economics* 16 (2020), 143 ff.

(197) This approach is also sufficiently flexible and responsive to cater to the dynamics of digital service platforms while providing considerable regulatory certainty to digital platforms.[194] Such asymmetric regulation is also unlikely to exacerbate the existing consolidation of power in the digital platform ecosystem.

6. Bringing an SGI Approach to Fruition: the Institutional Dimension

(198) Article 14 TFEU foresees that the principles and conditions necessary for an SGI to fulfil its missions can be established by the European Parliament and Council relying on the ordinary legislative procedure. It also however specifies that such legislation shall be without prejudice to the competence of Member States to provide, to commission and to fund SGI. This legal basis could be coupled with Article 114 TFEU, which enables the EU to adopt legislation to approximate the law, regulation or administrative practice of Member States in order to ensure the functioning of the Internal Market. These provisions, read in light of the principle of subsidiarity in Article 5 TEU, require an institutional and substantive division of labour between the European Commission and the authorities of EU Member States. The following model, or similar, may therefore be appropriate for the designation of services as SGI and the oversight of SGI obligations.

a) The designation of services as SGI

(199) At supra-national level, the European Commission or a new network comprised of representatives of national digital regulation networks could designate services as SGI. Where a platform service is not deemed essential at European level, but is deemed essential at Member State level (for instance, States where eGovernment services are already at an advanced stage of development), then Member States retain discretion to add to the list of SGI.

b) Oversight of SGI obligations

(200) Different elements of SGI obligations may relate more closely to the existing work of a single regulator: for instance, market-access requirements relate closely to the work of competition authorities while universal service obligations may be more closely aligned to the work of consumer protection authorities. There are therefore several options to consider when it comes to the oversight of compliance with obligations imposed on the envisaged SGI.

(201) At national level, there are three primary options:

---

194 This would alleviate concerns such as those raised in the Special Advisors' Report that 'in very fast moving and diversified markets' traditional utility style regulation (which organises the whole sector) is inappropriate. Special Advisors' Report, n 19, 19.

1. Consumer protection authorities could exercise oversight
2. Member States could be allowed and required to designate the appropriate domestic authority to exercise oversight
3. Mandate cooperation between existing relevant authorities at national level through a 'Digital Regulatory Network' or similar.

(202) Of these options, 3 is preferred. Option 1 is unduly narrow in focus given that the SGI obligations are likely relevant to several areas of law, and therefore the existing regulatory powers of several authorities. Option 2 has the benefit of maximising national institutional autonomy, as the Member State will be able to identify what authority is best suited for oversight. However, this also increases the chance of diverging approaches between Member States if some, for instance, appoint competition authorities to this role while others appoint data protection authorities. Option 3 would not require the creation of a new institution but would formalise cooperation between relevant agencies; cooperation that is already occurring in several Member States. This would also have the benefit of ensuring that a plurality of perspectives are taken into account when overseeing implementation of SGI obligations. It would also have the tangential benefit of promoting good working relationships between authorities, which may enhance the consistency between distinct bodies of law more generally.

(203) At European level, there are similarly three main options for oversight of national compliance:

1. By the European Commission
2. By a bespoke network of designated national regulators
3. By an existing network of regulators. This could be through the Consumer Protection Cooperation Network (CPC) or through the formalisation of a mechanism such as the Digital Clearing House, bringing together consumer protection, competition and data protection authorities, amongst others.[195]

(204) If each Member State coordinates the actions of its existing authorities through a Digital Regulatory Network, then Option 3 risks being either too narrow (by limiting European oversight to that undertaken by consumer protection authorities) or too broad (by bringing together several regulatory authorities from each State in the Digital Clearing House).

(205) The choice is therefore an open one between Option 2 or Option 1. Both present advantages and disadvantages. With regard to Option 2, the creation of a bespoke network of designated national regulators, this would ensure that the experience at national level in the domestic Digital Regulatory Networks was reflected at European

195 For further information on the existing "Digital Clearing House" structure, see here: https://www.digitalclearinghouse.org.

level. It would also create an institutional link between Member States, thereby potentially encouraging more harmonious approaches. On the other hand, existing experience of such regulatory networks is mixed. For instance, the European Competition Network functions effectively for the exchange of best practice and ensures a certain level of consistency in decision-making. However, it does not have binding decision-making powers. The European Data Protection Board (EDPB) responsible for transnational data protection oversight does have such powers however its effectiveness to date has been called into question.[196] As such, the safest option for oversight is Option 1: oversight by the European Commission. This presents the benefit of ensuring a certain uniformity of approach across the EU while national specificities could still be taken into account by ensuring close cooperation between the Commission and designated domestic points of contact.

VI. Conclusions and Recommendations

(206) This report has examined whether it is appropriate to extend the legal framework for SGI to digital platform services. It suggests that there are strong reasons to recognise the important societal role of platforms, beyond their economic impact. Given that their design and delivery shapes the digital public sphere in important ways, the report considers whether the market-based and universal service obligations imposed on SGI in other contexts might be relevant to the platform environment. It concludes that a number of these obligations would enhance the protection of individuals, as consumers and EU residents.

(207) Recommendations made include:

- the extension of systemic transparency obligations for algorithmic decision-making processes. This could include, for instance, the requirement of independent third party oversight of such processes on an ongoing basis or, less significantly the requirement that an audit trail be maintained of these processes for oversight purposes.
- mandating protocol interoperability requirements, while working to address some of the unresolved queries about the impact of federation on data protection and content moderation;
- the introduction of comparison tools, considering in particular the intensity of the use and sharing of personal data by the platform and the consumer's right to avoid that by paying a certain amount of money;

196 European Commission, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation', COM(2020) 264, 5.

- an obligation for platform operators to grant access to the platform to all interested consumers, and limitations to the suspension or termination of the service;
- the introduction of a choice requirement that would enable individuals to access digital services without personal data processing. This would not prevent the service being subsidised through contextual advertising.

(208) In order to oversee these regulatory requirements a hybrid supra-national/national institutional model could be foreseen. Transnational services could be designated as SGI by the European Commission, with the possibility left open for Member States to add to this list. The implementation of SGI obligations would be overseen at national level by a designated 'Digital Regulatory Network' made up of representatives of relevant agencies at national level. The European Commission would liaise with a representative from this designated agency to ensure Member State compliance with its obligations. Failure to comply with SGI obligations by an entity deemed an SGI would be sanctioned at national level through effective, dissuasive and proportionate remedies.

Published in March 2021 by BEUC, Brussels, Belgium.

BEUC-X-2021-018

The European Consumer Organisation
Bureau Europeen des Unions de Consommateurs
Europaischer Verbraucherverband
Rue d'Arlon, 80 Bte 1, B - 1040 Bruxelles

BEUC The European Consumer Organisation