European Review of Private Law 5-2021 [701–732]

A Consumer Law Perspective on the Commercialization of Data*

Mateja Durovic** & Franciszek Lech***

Abstract:Commercialization of consumers' personal data in the digital economy poses serious, both conceptual and practical, challenges to the traditional approach of European Union (EU) Consumer Law. This article argues that mass-spread, automated, algorithmic decision-making casts doubt on the foundational paradigm of EU consumer law: consent and autonomy. Moreover, it poses threats of discrimination and undermining of consumer privacy. It is argued that the recent legislative reaction by the EU Commission, in the form of the 'New Deal for Consumers', was a step in the right direction, but fell short due to its continued reliance on consent, autonomy and failure to adequately protect consumers from indirect discrimination. It is posited that a focus on creating a contracting landscape where the consumer may be properly informed in material respects is required, which in turn necessitates blending the approaches of competition, consumer protection and data protection laws.

Résumé: La commercialisation des données personnelles des consommateurs dans l'économie numérique pose de sérieux défis conceptuels et pratiques à l'approche traditionnelle du droit européen de la consommation. Cet article soutient que la prise de décision algorithmique automatisée et répandue en masse jette un doute sur le paradigme fondamental du droit européen de la consommation: le consentement et l'autonomie. En outre, elle présente des menaces de discrimination et d'atteinte à la vie privée des consommateurs. La réaction législative récente de la Commission Européenne, sous la forme du 'New Deal for Consumers', a été un pas dans la bonne direction, mais n'a pas été à la hauteur en raison de sa confiance continue dans le consentement et l'autonomie et de son incapacité à protéger adéquatement les consommateurs contre la discrimination indirecte. Il est proposé de se concentrer sur la création d'un paysage contractuel dans lequel le consommateur peut être correctement informé sur des aspects matériels, ce qui nécessite de combiner les approches des lois sur la concurrence, la protection des consommateurs et la protection des données.

Zusammenfassung: Die Kommerzialisierung der personenbezogenen Daten von Verbrauchern in der digitalen Wirtschaft stellt den traditionellen Ansatz des EU-Verbraucherrechts vor ernsthafte konzeptionelle und praktische Herausforderungen. Dieser Artikel argumentiert, dass die massenhafte Verbreitung automatisierter algorithmischer Entscheidungsfindung das grundlegende Paradigma des EU-Verbraucherrechts in Frage stellt: Zustimmung und Autonomie. Darüber hinaus birgt sie die Gefahr der

* This work is part of/contributes to the larger work undertaken by the author at the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN). The final version of this article was submitted on 28 July 2021.

** Dickson Poon School of Law, King's College London UK. Email: mateja.durovic@kcl.ac.uk.

*** Faculty of Law, University of Oxford.

Diskriminierung und Untergrabung der Privatsphäre der Verbraucher. Es wird argumentiert, dass die jüngste gesetzgeberische Reaktion der EU-Kommission in Form des 'New Deal for Consumers' ein Schritt in die richtige Richtung war, aber aufgrund des anhaltenden Verlassens auf Zustimmung und Autonomie und des Versagens, Verbraucher angemessen vor indirekter Diskriminierung zu schützen, zu kurz greift. Es wird postuliert, dass ein Fokus auf die Schaffung einer Vertragslandschaft erforderlich ist, in der der Verbraucher in wesentlichen Punkten ordnungsgemäß informiert werden kann, was wiederum eine Verschmelzung der Ansätze von Wettbewerbs-, Verbraucherschutz- und Datenschutzrecht erfordert.

1. Introduction

1. The right to the protection of personal data is a fundamental right recognized in the European Union (EU).[1] Despite its fundamental status, commercial and technological advances are rendering this right increasingly frail. Incidents such as the Facebook-Cambridge Analytica scandal, which exposed the extent to which the personal data of 87 million people could be collected, processed, and deployed without any prior consent to enfeeble our democratic process,[2] illustrate that we must be concerned about personal data protection as *citizens*. Yet these developments serve also as baleful admonitions that we must be concerned about the exploitation of our personal data as *consumers* – in the end, the agencies persecuting Facebook and imposing massive fines were the consumer protection bodies: the Federal Trade Commission (FTC) in the US, and the Information Commissioner's Office in the UK.[3]

2. The Cambridge Analytica scandal was an illustration of the extremes of the reality of Big Data, where our personal data is just another commodity: social network users, heretofore convinced that these digital services were free, realized that the price of access is their personal data, which is later monetized by these social network platforms. Furthermore, the scandal demonstrated how Consumer Protection Law, Privacy, Data Protection, algorithmic targeting, and Big Data technology are all interconnected.

---

1 Charter of the Fundamental Rights of the European Union, http://data.europa.eu/eli/treaty/char_2016/oj ('Charter'), Art. 8(1); Consolidated Version of the Treaty on the Functioning of the European Union, http://data.europa.eu/eli/treaty/tfeu_2012/oj ('TFEU'), Art. 16(1).

2 BBC News, *Facebook Scandal Hit 87 Million Users* (4 April 2018), https://www.bbc.com/news/technology-43649018 (accessed 2 March 2020).

3 FTC forced Facebook to pay a historic $5bn in fines and adopt a more transparent corporate structure in the aftermath, see FTC, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, Press Release (24 July 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions (accessed 2 March 2020). In the UK, the ICO imposed a more modest £500,000 fine on Facebook for the breaches of Data protection law in the course of the scandal, see ICO, *ICO Issues Maximum £500,000 Fine to Facebook for Failing to Protect Users' Personal Information* (25 October 2018), https://ico.org.uk/facebook-fine-20181025 (accessed 2 March 2020).

The cosmic challenge posed to Consumer Protection Law by the rise of algorithm-driven Big Data, also requires a veritable paradigm shift in the regulatory response; an approach which abandons the traditional focus on addressing bargaining imbalance in favour of a more interdisciplinary approach that unifies and blends the approaches of Data Protection, Privacy Protection, Competition and Consumer Protection Law.[4] To remain in disciplinary silos is to fatally undercut the law's ability to protect our consumer rights in the Big Data world.

3. This concern surrounding the application of Big Data technology to consumer transactions, on the fast evolving 'digital marketplace', prompted the EU to adopt a string of measures aimed at safeguarding the rights of both its citizens and consumers. This process has been massively accelerated during the Covid-19 pandemic, which forced consumers and traders alike to move onto the digital market place on a previously unprecedented scale.

The European Commission ('Commission') proposed a 'New Deal for Consumers'[5] – the reference to Franklin D. Roosevelt's 1930s momentous reforms hints at the size of the Commission's ambitions.[6] The professed aim of the New Deal for Consumers is to 'fill the gaps in the current consumer *acquis*' and to 'look at future challenges for consumer policy in a fast evolving economic and technological environment'.[7] Throughout the contribution, when we refer to the 'New Deal for Consumers', we are referring to the changes brought by the Commission in the Digital Content Directive (DCD) (Directive 2019/770), the Directive 2019/771 and the so-called 'Omnibus Directive' (Directive 2019/2161).[8]

The Commission's initiative was received with cautious enthusiasm: the European Data Protection Supervisor ('EDPS') 'welcomed' it, though the EDPS also emphasized 'the need to fill the gaps in the current consumer *acquis* in order to respond to the challenge presented by ... massive collection and monetisation of personal data'.[9] Likewise, the present contribution believes that the Commission's

---

4 Inge Graef, Damian Clifford & Peggy Valcke, 'Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law', 8. *International Data Privacy Law* 2018(3), p (200) at 202.

5 European Commission, *A New Deal for Consumers* (11 Apr. 2018), COM/2018/0183, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0183&qid=1625581969548 ('New Deal for Consumers Document').

6 For an overview see Mateja Durovic, 'Adaptation of Consumer Law to the Digital Age: The Case of the New European Directive 2019/2161 on Modernisation and Better Enforcement of Consumer Law', 68. *Annals of the Faculty of Law in Belgrade* 2020, p (62) at 67–76.

7 *A New Deal for Consumers Document*, pp 3–4.

8 Mateusz Grochowski, 'European Consumer Law after the New Deal: A Tryptich', 39. *Yearbook of European Law* 2020, p (387) at 389–390.

9 European Data Protection Supervisor, *Summary of the Opinion of the European Data Protection Supervisor on the Legislative Package 'A New Deal for Consumers'* (30 October 2018), p 69, [2018] *OJ* C 432/17, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018XX1130%2801%29&qid=1625582420564 ('EDPS Opinion').

New Deal is a step in the right direction, although by failing to liberate itself from the old paradigms of Consumer Protection, rooted in pre-Big Data realities, it fails to go sufficiently far.

4. Instinctively, the most relevant EU legislation on the matter of data collection is, of course, the General Data Protection Regulation of 2016 ('GDPR'),[10] but that is not the sole relevant legislation: the *acquis communautaire* has now also extended the protection of consumer protection laws to cover digital consumer transactions where personal data is commercialized.

Directive 2019/770 on the supply of digital content,[11] for example, extends traditional Consumer Law provisions[12] to contracts 'where ... the consumer provides or undertakes to provide personal data to the trader' in exchange of the digital service or content.[13] Furthermore, following the amendments introduced by Directive 2019/2161 on better enforcement and modernization of EU consumer protection, Consumer Law will now apply also to contracts concluded for 'free' digital services, where personal data is provided as consideration for digital services.[14] These adaptations, discussed more fully below,[15] mark the necessary transmutations that ordinary consumer law has to undertake in order to maintain relevance in the era of Big Data.

5. This legislative initiative highlights the crucial difficulty besetting the regulatory efforts undertaken by the EU: it is nigh impossible to design a regulatory response that safeguards commercial use (and the correlative consumer enjoyment) of disruptive and innovative technology, while preserving the fundamental rights of consumers; especially where technological innovation considerably outpaces the regulatory process.[16]

---

10 Regulation 2016/679 of 27 Apr. 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), http://data.europa.eu/eli/reg/2016/679/oj ('GDPR').

11 Directive 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, http://data.europa.eu/eli/dir/2019/770/oj ('Digital Content Directive' or 'DCD').

12 See Dir 2019/770, Arts 5-8 and 11-18.

13 Dir 2019/770, Art. 3(1).

14 Directive 2019/2161 of 27 Nov. 2019 amending Council Directive 93/13 and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, http://data.europa.eu/eli/dir/2019/2161/oj, Art. 4(2)(b); Directive 2011/83 of 25 Oct. 2011 on consumer rights, http://data.europa.eu/eli/dir/2011/83/oj ('Consumer Rights Directive' or 'CRD'), Art. 3(1a).

15 See below: s. 4.

16 Eric Vermeulen, Mark Fenwick & Wulf Kaal, *Regulation Tomorrow: What Happens When Technology Is Faster than the Law*, Tilburg University Discussion Paper DP-2016-024 (2016), p (1) at 5.

We submit that it is precisely for this reason that the regulatory approach taken by the Commission will never be wholly adequate. Still, the major issue is conceptualizing Consumer Law's response to this commercialization of consumers' personal data. In this contribution, we argue that the current EU response is a step in the right direction, but fails to go sufficiently far to protect consumer rights in the age of Big Data. Moreover, the New Deal for Consumers contains important shortcomings, which undermine legal certainty, and scuppers a seamless and interdisciplinary response by the EU *acquis* to the challenges thrown up by Big Data.

6. We proceed as follows: firstly, we explore the nexus between the rise of Big Data technology, and the process of commercialization of consumers' personal data. Secondly, we turn to analyse the risks raised by the widespread commercialization of consumer data, which we use to support the case for regulatory intervention to safeguard consumers' rights. Thirdly, we analyse how EU *acquis* has dealt with the protection of consumers' privacy, before turning to scrutinize the interplay between data protection and consumer protection regimes.

2. Big Data and Consumers' Information

7. First, we ought to clarify the key terms used. We understand 'commercialization of consumer data' to mean the act of trading with one's personal information, on the assumption that the personal data of a consumer has an economic value, which is transferred to the trader in exchange for the provision of content or a service.[17]

It may seem that this terminological point is trite, yet we believe that a significant conceptual point lurks behind it. Directives 2019/770 and 2019/2161 insist that the commercialization of consumer data refers to the act whereby consumers provide personal data to the trader in exchange for a service.[18] However, it would be more accurate to describe the actual benefit conferred by the consumer, in exchange for goods or services, to be the *consent* to data collection rather than the data *itself*.[19] After all, traders may have already been entitled to collect some data regarding the consumer; [20] the 'added' benefit is therefore the consumer permitting the trader to collect data beyond what the trader would have,

17 Carmen Langhanke & Martin Schmidt-Kessel, 'Consumer Data as Consideration', 6. *Journal of European Consumer and Market Law* 2015, p (218) at 219.

18 Dir 2019/770, Art. 3(1); Dir 2019/2161, Art. 4(2)(b).

19 Carmen Langhanke & Martin Schmidt-Kessel, 6. *JECML* 2015, p 222.

20 Even under the new regime see Dir 2019/770, Art. 3(1): This Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader, *except* where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive or for allowing the trader to

in the absence of further consent, already been legally entitled to collect. Hence when speaking of commercialization of consumers' personal data, we refer to the ability of consumers to exchange their consent to part with their personal data for a service or a good.

8. The commercial rationale for traders to accept a consumer's personal data as consideration is that the personal data received by the seller has an equal or superior economic value than the good or service provided. Value of data does not include exclusively its utility to the *collector*; it also includes the monetary value of passing that data further[21]: for example, a platform that intermediates transactions between sellers and buyers, can collect personal data to assemble customer profiles, which in turn present value for advertising companies (for example), which are eager to purchase them.

9. Another relevant trend is the increasing role of data-driven algorithms in commercial decision-making. This will deepen the dependence of commercial actors on Big Data for their future competitive advantage, and ultimately, commercial viability. At the intersection of these two trends: the growing value of personal data, and the increasing dependence on algorithms, lies the prospect of even more accelerated rate of the commercialization of consumer data in the near future. This helps to contextualize why discussing the consumer protection law's response to this phenomenon is so pertinent.

10. Secondly, we need to clarify what we mean by the ephemeral, and perhaps overused, phrase: 'Big Data'. Surprisingly, given the prominence that this term has in popular discourse, as well as in academic commentary, 'Big Data' does not have a fixed definition. The original definition characterized Big Data as 'data that contains greater variety arriving in increasing volumes and with ever-higher velocity'.[22] Some commentators focus on the fact that what makes data 'Big' is the 'use of technologies that can analyse data that are not centrally located, are not stored in a uniform format and are incomplete'.[23]

We on the other hand, throughout the present contribution, take 'Big Data' to mean 'gigantic digital datasets', analysed by algorithms,[24] taking advantage of the fact that the scope and purpose of our aim allows a certain degree of generality

---

comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose.

21 Juan Qi, 'Application of Essential Facilities Doctrine to "Big Data": US and EU Perspectives', 40. *European Competition Law Review* 2019, p (182) at 183.

22 Oracle, *What is Big Data?*, https://www.oracle.com/big-data/guide/what-is-big-data.html (accessed 6 July 2021).

23 Max N. Helveston, 'Consumer Protection in the Age of Big Data', 93. *Washington University Law Review* 2016, p (859) at 867.

24 Juan Qi, 40, *ECLR* 2019, p 182.

in applying the term. It is important to note that 'Big Data' refers to a combination of the technology and process. Technology is the hardware used to sift, sort and analyse mountains of data in milliseconds. The process is analysing the data into patterns and applying the patterns to predictive analytics to be then used on new data.[25]

3. Consumer Rights and Big Data: Threats

11. As a preface to the discussion of the threats that Big Data invariably poses, it is important to note that the commercialization of consumer data also has its benefits: it allows consumers access to services that would otherwise have to be paid for with traditional form of currency – meaning the nominal *pecuniary* cost is much lower thanks to the ability to commercialize personal data. However, this is a double-edged sword, as it relies on undermining of the *value* of personal data.[26] Moreover, the fact that initially such services were often advertised as 'free', with the real cost only emerging later, is legally considered to be an unfair commercial practice anyway.[27]

12. Another putative benefit of Big Data for consumers is increased efficiency: as companies benefit from more complete information on their target consumers, which permits more efficient targeting, potentially exposing consumers only to 'relevant' advertising. Economic theory then forecasts lower production and marketing costs, which could lead to lower prices. Moreover, Big Data can facilitate a more efficient matching between consumers and products and services resulting in higher consumer welfare.[28]

13. Furthermore, one could argue that efficiency would also be improved in certain areas where knowledge about the consumer is vital such as credit and insurance. Big Data will allow lenders and insurers to paint a holistic picture of the individual consumer and provide a service tailored to that specific consumer. In relation to credit, Big Data might enable some consumers to be given loans that would otherwise be refused on the basis of how they look in standard credit-worthiness ratings.[29]

---

25 Julie E. Cohen, 'What Privacy is For', 126. *Harvard Law Review* 2013, p (1904) at 1920.

26 See below s. 3.1.

27 Directive 2005/29 of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, http://data.europa.eu/eli/dir/2005/29/oj ('Unfair Commercial Practices Directive') ('UCPD'), Annex I, para. 20.

28 Wolfgang Kerber, *Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection*, No. 14-2016 Joint Discussion Paper Series in Economics (Philipps-University Marburg, School of Business and Economics 2016), p (1) at 4.

29 See Frederico Ferretti, 'Consumer Access to Capital in The Age of FinTech and Big Data: The Limits of EU Law', 25. *Maastricht Journal of European and Comparative Law* 2018, p (476) at 486-487.

14. Yet, despite these potential gains, the threats to consumers created by the increased commercialization of their personal information[30] are definitely serious. Sufficiently serious, in fact, to warrant consumer protection law's response to the contingency. In the present section we take a look at the most significant of the threats linked with this increased commercialization of personal data of consumers.

3.1. Value

15. The value of personal data, which consumers provide to traders, may actually be impossible to calculate precisely.[31] In any event, individual consumers will, most likely, be completely unaware of the value of the data they make available in exchange for goods or services. When our data is taken and sold as a part of a broader database, or as a consumer profile, its commercial value is determined by calculations independent of us *qua* individual consumer. Consequently, even the most vigilant consumer may be unaware of the actual *value* of the data they are conferring to a trader under a consumer contract.[32]

16. In this context, the lack of awareness as to the value of the counter-performance creates fertile ground for the consumer to be taken advantage of. This threat may seem trivial in comparison to the dystopian danger consumers are accustomed to expect from the 'Big Data Revolution', but it remains a profoundly significant one.

17. Due to this difficulty with estimating the value of the consideration that is supplied by the customer, the EU consumer *acquis* must undergo a paradigm shift: its norms ought not merely protect the integrity of the consumer, or simply address the imbalance of bargaining power, but rather, they must also protect the proprietary interest and economic preferences of consumers in their own personal data.[33]

Traditionally, the focus of consumer protection law was not about ensuring that a consumer got a 'good deal', or that the consumer received adequate value for the consideration they provided, so long as the relevant provision was expressed in plain and intelligible language.[34] The Big Data revolution however, will require the consumer protection regime to move beyond its traditional jurisdiction, and actually scrutinize the value exchanged, if it is to achieve its more fundamental goal of addressing the inequality of bargaining power in consumer contracts.

---

30 GDPR, Recital 6.

31 EDPS Opinion, *Summary of the Opinion*, p 72.

32 Carmen Langhanke & Martin Schmidt-Kessel, 6. *JECML* 2015, p 219.

33 Carmen Langhanke & Martin Schmidt-Kessel, 6. *JECML* 2015, p 222.

34 See e.g., Directive 93/13 of 5 Apr. 1993 on unfair terms in consumer contracts, http://data.europa.eu/eli/dir/1993/13/oj ('Unfair Contract Terms Directive'), Art. 4(2); ECJ 30 Apr. 2014, ECLI:EU:C:2014:282, *Kásler* v. *OTP Jelzálogbank Zrt*, curia.europa.eu/juris/documents.jsf?num=C-26/13, p 68.

18. One way of achieving this shift is for consumer protection law to take a leaf out of data protection law's book. Under the GDPR, data subjects have the right to data portability,[35] which gives the data subjects 'control' over their own personal data.[36] Thus, the GDPR seeks to address the imbalance between the data subject and controller. Substitute consumer and trader for data subject and controller, and the two regimes may be working in tandem. Moreover, a competitive digital single market, requires not only the free movement of data (which GDPR aspires to provide),[37] but must also address the dominant market position of the digital service behemoths (Google, Facebook, etc.), which gives them a controlling-position in the market.

Hence, the goal of empowering the consumer in the world where their personal data is a medium of exchange, must adequately safeguard the proprietary and monetary value those consumers hold in their data. Accordingly, it seems that EU law must coordinate its 'consumer protection response', with a concurrent integration of data protection and competition law responses.

19. However, at the moment EU *acquis* falls considerably short in this regard. The new Directive 2019/2161 merely states that 'processing of personal data should comply with [the GDPR]'.[38] It is difficult to speak of a coordination between the two Acts: the hierarchy between them is not specified, meaning that protection offered by the GDPR may be undermined by the consumer protection directives.

The mere mention of the GDPR is a welcome step, but in itself is insufficient. For starters, the broad definition of 'data subject',[39] 'data processing'[40] and 'data controller'[41] provided by the GDPR means that there is an ample ground for

35 GDPR, Art. 20.

36 GDPR, Recital 7.

37 GDPR, Art. 1(3).

38 Dir 2019/2161, Recital 33.

39 GDPR, Art. 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; also ECJ 16 Jan. 2019, ECLI:EU:C:2019:26, *Deutsche Post AG* v. *Hauptzollamt Köln*, curia.europa.eu/juris/documents.jsf?num=C-496/17, pp 54-55.

40 GDPR, Art. 4(2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

41 GDPR, Art. 4(3): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

overlap between two regimes: after the consumer provides their personal data to the trader in exchange for services or content, the trader will become a 'controller' and so the GDPR will apply. Since the GDPR and the new Directive 2019/2161 provide divergent rights and protections,[42] a precise regime for the interaction of the two regimes is required to ensure that the GDPR rights are not undermined.

20. It is argued that the GDPR should operate as the foundation document, setting out the minimal rights of data subjects; indeed, the Recitals in the Preamble to the GDPR corroborate this goal.[43] The Consumer Protection Directives, consequently, should expressly provide that the GDPR is the overarching document. Any attempt to create a vibrant, internal data market, conducive of development of a digital economy,[44] will be frustrated without a clear protection of consumers' proprietary interest in their personal data by consumer law, which in turn is not possible without coordination between the GDPR and the New Deal for Consumers.

3.2. Security Breaches

21. The inevitable consequence of the increased commercialization of consumers' personal data is that data processing entities *qua* traders, will be forced to store colossal amounts of personal data on their servers. This in turn will render them enticing targets for hackers.

The risk of sensitive data thefts and leaks is rarely the most prominent on the list of problems associated with Big Data, and yet some, including Vladeck, label this security threat as '*the* most urgent ... and the most disruptive' element of the Big Data economy.[45] Experts draw attention to a 'meteoric' increase of identity theft, which they label as 'predictable debris of an Internet economy that places too little value on data security'.[46]

In the US, where the consumer protection and data protection regimes are less comprehensive than in the EU, the FTC has received over 330,000 complaints relating to identity theft alone; the Department of Justice approximated that 7% of US Population of people aged over 16 have been victim of some form of identity theft.[47]

---

42 See below s. 4.

43 GDPR, Recital 11: [The GDPR aims to] 'set out in detail the rights of data subjects and the obligations of those who process and determine the processing of personal data'.

44 GDPR, Recital 7.

45 David C. Vladeck, 'Consumer Protection in an Era of Big Data', 42. *Ohio Northern University Law Review* 2016, p (493) at 500; Max N. Helveston, 93. *WULR* 2016, p 873.

46 David C. Vladeck, 42. *ONULR* 2016, p 500.

47 David C. Vladeck, 42. *ONULR* 2016, p 500.

22. Despite this exponential increase, the FTC has brought only 60 enforcement actions against entities that failed to have reasonably secure methods of storing data. This spasmodic enforcement method undermines the deterrence effect, and fails to incentivize data controllers to invest in cybersecurity. Vladeck suggests that the cause for this lack of effectiveness is that the FTC is limited to forward-looking injunctions, and lacks authority to impose civil penalties,[48] which suggests that the lesson to be drawn by regulators around the globe is that data security requires effective enforcement mechanisms vis-à-vis data controllers.

23. Meanwhile in Europe, the EU legislator has been paying attention. Directive 2019/2161 lays emphasis on enforcement; crucially, it increases the penalties that may be imposed on incompliant traders.[49] This is indeed a welcome development, which may allow the EU regulators to motivate (using the stick rather than the carrot if necessary) data-controlling traders to keep the consumers' personal data safe. Whether this is by itself sufficient to stave off the challenge posed by the increased levels of data collection is unlikely.

24. The picture that emerges is that with the rise of Big Data, more personal information will be collected and stored, which means that more personal information is susceptible to be stolen and misplaced.

Furthermore, consumers lack effective redress against the companies and unwinding the damage caused by identity theft can be both cumbersome and expensive. This is compounded by the fact that increasingly more intimate information is being collected – our phones, TVs and even fridges and washing machines are listening to private conversations.[50]

25. The consequence is that consumers are more susceptible to be harmed by mistreatment or theft of their personal data. There remains an absence of transparency of how the data is collected, stored and analysed.[51] If the consumers are to consent to the increased processing of their data for traders' purposes, it is desirable, though by no means certain,[52] that they should be sure that their personal information is safe.

---

48 David C. Vladeck, 42. *ONULR* 2016, p 506.

49 Dir 2019/2161, Recitals 11–14 and Arts 1, 2(2), 3(6), 4(13).

50 David C. Vladeck, 42. *ONULR* 2016, p 499.

51 Inge Graef, Damian Clifford & Peggy Valcke, 8. *IDPL* 2018, p 202.

52 Susan Athey, Christian Catalini & Catherine E. Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*, No 5196-17 MIT Sloan Research Paper (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2916489, p 2; Wolfgang Kerber, *Digital Markets, Data and Privacy*, p 6.

3.3. Inability of Traders to Faithfully Rely on Consumers' Consent

26. Data protection laws were initially seen as a defence against privacy violations of the State,[53] with their extension to a data collection and processing by private entities occurring later.[54] Perhaps it is for this reason that societies generally tend to rely on the mechanism of consent to regulate the types of data that can be collected and processed. The increased commercialization of consumers' personal information means that the mechanism of consent, as presently conceptualized and applied, is no longer adequate and needs to be enhanced, through the informational and remedial empowerment of the consumer.[55]

27. However, the New Deal for Consumers, as exemplified by Directive 2019/2161, not only continues to rely on the notion of consent but actually reinforces the central place which consent occupies. If we are right to see the reliance on the consent as inadequate, then the new regime is just as vulnerable as the old regime in protecting the fundamental rights of consumers in the Big Data reality.

28. The central role of consent in the data protection regime is evident. Article 6 of the GDPR provides that processing of data is 'lawful only if and to the extent' that, inter alia, 'the data subject has given consent to the processing of his or her personal data'.[56] Consent is defined as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which [they], by a statement or by a clear affirmative action, signif[y] agreement to the processing of personal data relating to [them]'.[57] Furthermore, Article 7 of the GDPR provides conditions for valid consent, specifying that the request for consent should be presented in

---

53 See e.g., High Court, Chancery Division 28 Feb. 1979, *Malone* v. *Metropolitan Police Commissioner* [1979], Ch. 344, https://www.bailii.org/ew/cases/EWHC/Ch/1979/2.html, pp 372–374 (Megarry V-C); ECtHR 2 August 1984, 8691/79 *Malone* v. *United Kingdom*, http://hudoc.echr.coe.int/eng?i=001-57533, pp 64–82. Although note James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty', 113. *Yale Law Journal* 2004, p 1151, who lucidly argues that the (Continental) European notions of privacy revolve around being 'spared embarrassment or humiliation', which makes the media the prime danger, whereas the US privacy protections focus on liberty and liberty against the state. In this dichotomy, English Data protection laws, on which we rely to make the above point, evidently developed in a way closer to the US model rather than the Continental model. Perhaps because English jurists were heavily involved in drafting the European Convention of Human Rights, its provisions (Art. 8) reflect the value of privacy as conceived in liberty against the state, and indeed early interpretations of privacy was conceived in this light. Many thanks to the Journal's anonymous reviewer for alerting us to this point.

54 Wolfgang Kerber, *Digital Markets, Data and Privacy*, p 14.

55 See GDPR, Recital 7.

56 GDPR, Art. 6(1)(a).

57 GDPR, Art. 4(11); ECJ 1 Oct. 2019 ECLI:EU:C:2019:801 *Planet49* v. *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV*, https://curia.europa.eu/juris/liste.jsf?num=C-673/17, pp 61–63.

plain and clear language, in 'intelligible' and 'easily accessible' form, and be distinguishable from consent as to other matters.[58] The emphasis on free will in giving consent is evident also from the Recitals to the GDPR, which state that consent should not be regarded as freely given if the data subject 'is unable to refuse or withdraw consent without detriment'[59] or 'where there is a clear imbalance between the data subject and the controller'.[60,61]

Two further important rights are enshrined in Article 7 of the GDPR: the right to withdraw consent at any point,[62] and a stipulation that in assessing the quality of consent account must be taken of whether the performance of a contract was conditional on consent to the processing of data.[63]

It is of interest to note the intersection of the GDPR-provided rights with the more general rights existing under the consumer law regime. Under Directive 2011/83 ('Consumer Rights Directive (CRD)'), consumers have a general right to withdraw from any off-premises contract[64] within 14 days,[65] upon which the mutual obligations of the parties cease to bind.[66] Meanwhile, as noted above, Article 7(2) of the GDPR provides a right of the data subject (consumer) to withdraw consent to data processing, while Article 20 GDPR allows 'data portability', that is, the right to 'receive the personal data ... in a structured, commonly used and machine-readable format' and to 'transmit those data to another controller'. In the context of contracts where the consumer's personal data was provided as a consideration for a good or a service the GDPR rights seem to complement the pre-existing rights under the CRD. At the same time, the withdrawal of consent for data processing under Article 7(2) GDPR may be interpreted as withdrawal of the consumer contract under the CRD. In light of a lack of a legislative hierarchy, the interaction of the two regimes will need to be fleshed out.

29. Notwithstanding, the insights regarding the role of consent in the GDPR become important when we compare consumer protection's 'fairness test' with data protection law's 'consent test'. It is useful to note here the similarity of the language in Recital 43 of the GDPR and Article 3 of the Unfair Contract Terms Directive.[67]

---

58 GDPR, Art. 7(2).
59 GDPR, Recital 42.
60 GDPR, Recital 43.
61 Frederico Ferretti, 25. *MJECL* 2018, p 496.
62 GDPR, Art. 7(3).
63 GDPR, Art. 7(4).
64 Dir 2011/83, Art. 2(8).
65 Dir 2011/83, Art. 9(1).
66 Dir 2011/83, Art. 12.
67 Unfair Contract Terms Directive 93/13, Art. 3(1): 'A contractual term ... 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'. (Emphasis supplied).

Due to the central role of consent, if the consumers are not actually in a position to give full and informed consent, or if the traders are unable to faithfully rely on consumer consent, the structure could crumble. Where provision of data is the counter-performance for the contract, if the trader is unable to validly rely on that consent, they legally cannot receive the counter-performance for their service, which means that the contract loses its commercial value. This in turn removes any motivation for the trader to trade with the consumer, and thus not only produces a chilling effect on technological innovation, but actually limits consumer choice.

30. The risk that data, when exchanged between collecting and data-processing entities, is reformatted for analysis and merged with other data – creates a feasible possibility that the consumer's personal data will be 'disassociated from information about its origins and permissible uses'.[68]

Furthermore, this dynamic of data processing makes it difficult to conform with the consent requirements because data compiled for one purpose may be merged with other data and then processed with another purpose in mind, thus making the initial consent, unless expressed very generally (which would in any event fail the 'fairness' test), inoperative. In this fast-paced technological realm, the notion of consent is 'elusive', because consumer's assent cannot be disassociated from the commercial reality against which they contract – that is superior bargaining power of the trader, especially in sensitive fields of insurance or credit, meaning that consumers may have no choice but to consent to collection of private data, on terms desired by the trader, rendering the 'consent' thus obtained but an empty shell.[69]

31. On top of this, data is increasingly collected through sensors and machines that have no interface with consumers, so there is no chance to give the consumers notice or obtain their consent to data collection.[70] Additionally, the exponential rise in the amount of personal data collected make it more unlikely that consumers' consent-based restrictions on the use of their data will be respected.[71]

32. Lastly, there is also the problem of consumers themselves. Surveys have shown that a 'large majority' of internet-users professes to be 'very concerned' about their privacy and personal data on the internet; yet, in reality those same consumers 'are not cautious about disclosing private information' online.[72] Especially where obtaining a service is conditional on providing data, consumers

68 Max N. Helveston, 93. *WULR* 2016, p 875.
69 Frederico Ferretti, 25. *MJECL* 2018, p 496.
70 David C. Vladeck, 42. *ONULR* 2016, p 507.
71 Max N. Helveston, 93. *WULR* 2016, p 864.
72 Wolfgang Kerber, *Digital Markets, Data and Privacy*, p 6.

'willingly consent or disclose information about themselves and their social activities without thinking about the effects of their disclosures'.[73]

These empirical trends undermine the law's insistence on consent as the organizing principle of protection. Athey et al., ran a series of scientific experiments on the Massachusetts Institute of Technology (MIT) Bitcoin club – they concluded that people are influenced by small incentives to prompt disclosure, a fact which they saw as explaining the privacy paradox of people declaring they care about privacy but disclosing private information quite easily when incentivized to do so.[74] This would mean that consumers are not fulfilling their 'moral obligation to respect ... other's people privacy but also their own', failing to notice the tremendous value of privacy in our societies and instead choosing to discard it easily.[75]

33. This point is central because it challenges the basic assumption underpinning EU's consumer and data protection law: the existence of an empowered, 'smart' consumer. Commentators argue that faced with Big Data, policymakers have a dilemma between empowering consumers themselves, or increasing state paternalism and regulation. The EU (through the GDPR, the Digital Services Directive and the Payment Services Directive[76]) has selected the path of consumer empowerment, which choice is to be applauded.[77] However, once we appreciate that consumers have not yet undergone the 'paradigm shift' from ordinary consumers into the 'Smart Digital Consumers' who wield their own sword and shield, then reliance on the consumers to protect themselves may not seems doomed to fail.

3.4. Discrimination

34. Much like the right to privacy and data protection, the right to not be subject to unlawful discrimination is also a fundamental right in the EU.[78] The fear at this juncture is firstly, that Big-Data-driven commercialization of consumers' personal data will create an environment where direct and indirect discrimination, especially on the basis of gender or race, is possible, and secondly, that any such discrimination will be impossible to detect (and thus to correct, prevent, or remedy).

Indeed, the fear was deemed sufficiently pressing that the Culture and Education Committee of the European Parliament passed a resolution requiring

---

73 Frederico Ferretti, 25. *MJECL* 2018, p 492.

74 Athey, Catalini & Tucker, *The Digital Privacy Paradox*, p 2.

75 Anita L. Allen, 'Protecting One's Own Privacy in A Big Data Economy', 130. *Harvard Law Review* 2016, p (71) at 72.

76 Directive 2015/2366 of 25 Nov. 2015 on payment services in the internal market, http://data.europa.eu/eli/dir/2015/2366/oj ('Payment Services Directive' or 'PSD').

77 Giuseppe Colangelo & Mariateresa Maggiolino, 'From Fragile to Smart Consumers: Shifting Paradigm for the Digital Era', 35. *Computer Law & Security Review* 2019, p (173) at 181; Wolfgang Kerber, *Digital Markets, Data and Privacy*, p 17.

78 Charter, Art. 21; TFEU, Art. 10.

artificial intelligence (AI) in the EU to be trained to prevent discrimination.[79] Discrimination-related risks, from government scoring, to hiring biases, to preventing access to credit, were all ranked as 'unacceptable' or 'high' risks by the Commission – indeed, the Commission has suggested that algorithmic discrimination is *the* main risk of AI, which must be counteracted.[80]

35. It is crucial to disambiguate between two meanings in which an algorithmic decision may be considered '*discriminatory*'. In the first sense, 'discriminatory' may simply refer to the fact of making a distinction between two similar cases. In the second, legal-technical sense, 'discriminatory' refers to a prejudicial distinction made between two individuals on the basis of a protected characteristic, such as race, gender, religion, sexual orientation, age, etc. Discrimination in this second sense is unlawful.[81]

36. Algorithmic decision-making is *inherently* discriminatory in the first sense, while also carrying a heightened risk of perpetuating indirect discrimination of the unlawful kind. This is because from the technical standpoint the data used in modelling the algorithm can never be fully free from bias, it, most frequently, over-represents some classes of data.[82] Furthermore, algorithms fed by Big Data decide on correlation and not causation[83]; accordingly, the algorithm may make a decision regarding an individual consumer based on the past behaviours not of that individual consumer, but rather of others. Indeed, given the ends with which predictive algorithms are designed, the 'most appropriately designed algorithm' is that which 'can select, or discriminate [in the first sense] most effectively'.[84]

Where this un-problematic differential treatment may take a turn towards the prejudicial and illegitimate discrimination is in conflating certain factors (such as lower credit rating, intellectual property (IP) address, lower chances of future income etc.) with a protected characteristic under anti-discrimination legislation

---

79 European Parliament, *AI Technologies Must Prevent Discrimination and Protect Diversity* (16 Mar. 2021), https://www.europarl.europa.eu/news/en/press-room/20210311IPR99709/ai-technologies-must-prevent-discrimination-and-protect-diversity (accessed 6 July 2021).

80 European Commission, *On Artificial Intelligence – A European Approach to Excellence and Trust*, White Paper COM(2020) 65, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, p 10.

81 ECJ 13 Dec. 1984 ECLI:EU:C:1984:394 *Seremide SpA* v. *Cassa Conguaglio Zucchero*, https://curia.europa.eu/juris/showPdf.jsf?text=&docid=92578&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=25739267, p 28. See e.g., Dir 2000/78 of 27 Nov. 2000 establishing a general framework for equal treatment in employment and occupation, http://data.europa.eu/eli/dir/2000/78/oj, Arts 1, 2(1), 4(1); ECJ 14 Mar. 2017 ECLI:EU:C:2017:204 *Bougnaoui* v. *Micropole SA*, curia.europa.eu/juris/documents.jsf?num=C-188/15, pp 26, 31–37.

82 Ljupcho Grozdanovski, 'In Search of Effectiveness and Fairness in Proving Algorithmic Discrimination in EU Law', 58. *Common Market Law Review* 2021, p (99) at 100.

83 David C. Vladeck, 42. *ONULR* 2016, p 495.

84 Frederico Ferretti, 25. *MJECL* 2018, p 492.

(race, gender, religious belief, etc.). As algorithmic decision-making is proliferated in the age of Big Data, so the risk grows that its prejudicially discriminatory nature may serve to effectively exclude some social groups from given goods and services, only exacerbating the ostracism of those vulnerable groups.

37. Sometimes the distinction is put as one between intentional and unintentional prejudicial discrimination. Intentional discrimination, which involves deliberate disparate treatment motivated by a protected characteristic (for example intentionally excluding individuals of a given sexual orientation from the business' premises) is of course illegal under EU law and unlikely to be willingly replicated by algorithms of commercial actors. Unintentional discrimination (sometimes called *disparate impact* as opposed to disparate treatment) on the other hand occurs where an ostensibly neutral characteristic (such as home ownership) acts as a proxy for a protected characteristic (such as race).[85]

In the context of Big Data, even if we ensure that the actual algorithm is not designed to engage in intentional discrimination,[86] the risk remains that it will practice unintentional discrimination. Neutral variables may become correlated with protected characteristics, making actual algorithm-dictated outcomes vary by race or gender in an illegitimate way.[87]

To illustrate, in the case of a recruitment algorithm, the data pool used may show that most of the high-performing employees (defined by frequency of bonuses) in a given industry are male – using this data the algorithm would associate work performance with gender and give preference to male applicants, perpetuating the stereotype that high-achievers are male.[88] Alternatively, a credit ranking algorithm may associate poor credit ranking with a given postcode, which in turn may effectively redline the inhabitants of the poor areas populated by a given racial minority, further exacerbating the poverty trap in those very neighbourhoods.

These are not mere speculations. In 2018, Amazon was forced to scrap its AI recruiting algorithm after they uncovered that the algorithm discriminated against women. Based on the data it was fed, which reflected the predominance of men in the tech industry, it penalized words in curriculum vitae (CV)s which related to females, as in 'women's chess club', for example, thus leading to lower relative rankings for female candidates.[89]

---

85 Andrew Burt, *How to Fight Discrimination in AI*, Harvard Business Review (2020), https://hbr.org/2020/08/how-to-fight-discrimination-in-ai (accessed 6 July 2021).

86 GDPR, Art. 9(1).

87 Talia Gillis & Jann Spiess, 'Big Data and Discrimination', 86. *University of Chicago Law Review* 2019, p (459) at 469.

88 Ljupcho Grozdanovski, 58. *CMLR* 2021, p 100.

89 Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, Reuters (11 October 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-

Nor are these practices limited to hiring algorithms – research shows that facial recognition software also suffers from race and gender biases, being substantially less able to recognize dark-skinned and female faces as opposed to white and male ones.[90] Selbst, in his comprehensive study of predictive policing in the United States, illustrated how Big Data analytics may result in 'new discrimination': the reproduction and exacerbation of 'the existing discrimination in society' as a result of the design choices in the algorithms.[91] He cites the examples of Google's AdWords systems that linked 'black-sounding' names to criminal records, or Amazon who unintentionally excluded ethnic-minority neighbourhoods from same-day delivery.[92] Selbst's empirical research demonstrates that despite the claims of the Big Data enthusiasts, it is not a panacea to modern forms of social and commercial exclusion.

Naturally those faults are not embedded in the concept of an algorithm, but rather are the result of data pools used to model them. Still, without ensuring that disparate impact on the basis of protected characteristics is not perpetuated by algorithms, the Big Data revolution may bring increased levels of illicit discrimination. This is compounded by the opacity of the actual workings of the algorithm, which severely restricts the ability to prove (and remedy) discrimination under the current legal framework,[93] and also by the fact that it is often extremely challenging to rid the data pools of hidden links and proxies for protected characteristics.[94]

38. Big Data's unfeeling pattern-driven, correlation-based decision-making may end up not only exacerbating pre-existing indirect discrimination, but also creating entirely novel forms of illicit discrimination. Individuals who do not conform to the predictive 'good' pattern of behaviour may be excluded from certain services by the algorithm. The fact that consumer transactions are moving to the digital market means that this sort of consumers' profiles may be applied instantly in an algorithmic price-setting mechanism meaning that it may be possible for consumers from certain backgrounds to face higher prices for the same goods or services, a risk that is especially apparent as pertains to credit or insurance.[95]

---

insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G (accessed 6 July 2021).

90 Joy Boulamwini, *Artificial Intelligence Has a Problem with Gender and Racial Bias. Here's How to Solve It*, Time (7 Febuary 2019), https://time.com/5520558/artificial-intelligence-racial-gender-bias/ (accessed 6 July 2021).

91 Andrew D. Selbst, 'Disparate Impact in Big Data Policing', 52. *Georgia Law Review* 2017, p (109) at 120.

92 Andrew D. Selbst, 52. *GLR* 2017, p 120.

93 Ljupcho Grozdanovski, 58. *CMLR* 2021, p 134.

94 Andrew Burt, *How to Fight Discrimination.*

95 Wolfgang Kerber, 'Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection', 11. *Journal of Intellectual Property Law and Practice* 2016, p (856) at 858.

39. This risk of algorithmic indirect discrimination is particularly acute since it creates an insurmountable barrier for some people to access vital services, such as credit, which in turn may effectively accelerate the rise of inequalities and the stratification of societies. A response which tries to *ex ante* delineate and exclude from algorithmic decision-making *any* data that may be interpreted or represent protected characteristics requires clairvoyance and borders on theoretically impossible.[96]

4. EU Consumer *Acquis* v. Commercialisation of Big Data

40. The EU is committed to a high degree of consumer protection.[97] For this commitment to be anything but empty words, the consumer protection regime must be adapted to the threats outlined above. However, the difficulties encountered by community legislators, as well as the shortcomings of their adopted responses, highlight the difficulty of effective regulation of such a fast-paced area.

Commercialization of consumer data is progressing too fast for Brussels to keep up, and so a different approach may be warranted. Rather than attempting to empower the consumer by requiring them to give 'informed' consent, creating an environment where the consumer would be so empowered should be the preferred approach.

4.1. Privacy and Consent

41. To begin with, EU's regulatory response to the commercialization of consumers' personal data is *conceptually* flawed, due to its reliance on the notion of consent. Consent is a '*central feature* underlying EU data protection law'.[98] True, under the GDPR, consumer consent is only one of the six possible bases for lawful data collection,[99] but it is the broadest one, making it the most often invoked one. Consequently, technological developments which cast doubt on the viability of consent, as the distinguishing factor between permissible and impermissible data collection and processing, may render EU's protective regime futile.

42. GDPR's provisions on consent[100] have been interpreted by Advocate General Szpunar to mean that consent must not only be informed and freely given, but also 'separate', that is different and separate to the activity of merely using a website for

96 Talia Gillis & Jann Spiess, 89. *UCLR* 2019, p 470.

97 TFEU, Art. 169(1); Charter, Art. 38.

98 Opinion of AG Szpunar 4 March 2020 ECLI:EU:C:2020:158 *Orange Romania SA* v. *National Authority for the Supervision of the Processing of Personal Data* at [36]; Opinion of AG Szpunar 21 Mar. 2019 ECLI:EU:C:2019:246 *Planet49 GmbH* v. *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.*V, p 57 (emphasis added).

99 GDPR, Art. 6(1).

100 GDPR, Recital 32, Arts 4, 6 & 7.

example.[101] The Court of Justice of the European Union (CJEU) agreed that a pre-ticked box that must be deselected by the consumer in order to withdraw their consent is not sufficient.[102] Advocate General Szpunar saw these provisions as establishing that for the purpose of convincing a court that consent is valid there 'must not be any room *whatsoever for any doubt* that the data subject was sufficiently informed' of all the circumstances surrounding the data processing and its consequences.[103]

This seems to set a rather high standard to both how informed and free the consumer must be when giving consent. Putting aside questions of feasibility of such a high degree of information, it seems pretty uncontroversial that Community law places values such as individual autonomy and self-management at a pedestal through its emphasis of consent.

43. The strong reliance on individual control, consent and self-management of data is not confined exclusively to data protection law either – within the sphere of consumer law, the Digital Content Directive stresses that GDPR's consent requirement applies in consumer contracts,[104] which explains why the GDPR remains so crucial even outside the narrow remit of data protection.

Additionally, the notion of consent and self-management for consumers is visible in the older statutes. For example, the Directive 2005/29 on unfair commercial practices prohibits[105] misleading and aggressive commercial practices on the ground that they 'cause or [are] likely to cause [the consumer] to take a transactional decision that [they] would not have taken otherwise'.[106] The argument seems to be that such unfair practices deprive the consumer of their *individual autonomy* and self-control that they would otherwise be able to exercise. CJEU has strengthened this interpretation holding that the concept of 'misleading' for the purposes of Unfair Commercial Practices Directive (UCPD) is to be understood as depriving the consumer of an opportunity to make an 'informed' choice.[107] Hence this idea of Consumer protection law as ensuring the autonomy of consumers is prevalent across the EU *acquis*.

44. This policy decision stems from the change in our contemporary understanding of 'privacy'. The 21st century has forced us to revise our traditional

---

101 Opinion of AG Szpunar 2019 C-637/17 *Planet49*, p 66.

102 ECJ 1 Oct. 2019, *supra* n. 57, *Planet49*, pp 61-63.

103 Opinion of AG Szpunar 4 Mar. 2020, *supra* n. 98, *Orange Romania*, pp 46–47 (emphasis supplied).

104 DCD, Recital 24.

105 Unfair Commercial Practices Directive, Art. 5(1).

106 Unfair Commercial Practices Directive, Arts 6(1), 7(1) & 8(1); see Mateja Durovic, *European Law on Unfair Commercial Practices and Contract Law* (Oxford: Hart Publishing 2016).

107 ECJ 7 Sept. 2016 ECLI:EU:C:2016:633 *Vincent Deroo-Blanquart* v. *Sony Europe Ltd*, curia.europa.eu/juris/documents.jsf?num=C-310/15, p 45; ECJ 19 Dec. 2013 ECLI:EU:C:2013:859 *Trento Sviluppo Srl* v. *Autorità Garante della Concorrenza e del Mercato*, curia.europa.eu/juris/documents.jsf?num=C-281/12, pp 31–33.

understanding of privacy as the 'right to be left alone'[108] and instead adopt a more complex definition. Stefano Rodotà has argued that privacy must be understood as a right to 'keep control over one's own information and determine the manner of building up one's own private sphere'.[109]

This idea has come to be known as the right to 'informational self-determination', and the German Federal Constitutional Court has justified the requirement of an individual being protected from 'unlimited collection, storage, use and sharing of personal data' back in the 1980s as being necessary to ensure 'the free development of one's personality'[110] under the provisions of the German Basic Law.[111] Rodotà stressed that the right to informational self-determination ought to encompass both inward (right not to know) and outward (to be kept off others' hands) data.[112]

In the US, Julie Cohen argued that privacy is 'shorthand for breathing room to engage in the processes of boundary management that enable and constitute self-development' – privacy fosters '(partial) self-determination'.[113] This idea bears strong resemblance to Rodotà's keeping control over one's own information and control over private sphere. She argues that lack of privacy reduces the scope for self-making, which could be seen as analogous to losing one's ability to exercise informational self-determination.[114]

45. Consent thus can be seen as underpinning the whole idea of privacy. Since the right to informational self-determination provides a right to decide what information is disclosed, and how it is used vis-à-vis the consumers, the logical requirement for that right to be of any substance is that consumers are in a position to decide and give informed consent.

EU legislators decided to stick with the notions of bolstering individual autonomy of the consumer that have historically formed the bedrock of consumer protection law, without stopping to ask if it is the right policy in response to the age of commercialization of personal data.[115] Elettra Bietti has argued that this

---

108 Samuel Warren & Louis Brandeis, 'The Right to Privacy', 4. *Harvard Law Review* 1890, p (193) at 196–205.

109 Stefano Rodotà, *'Data Protection as Fundamental Right', Reinventing Data Protection, International Conference* (Bruxelles 12–13 October 2007), p 2.

110 BVerfG, 15 Dec. 1983, https://www.bundesverfassungsgericht.de/EN/Entscheidungen/Entscheidungen/Entscheidungen.html;jsessionid=A64A857F600B41ED0D724B3770B004DB.2_cid383.

111 Article 2.1 of the Basic Law for the Federal Republic of Germany (right to free development of one's personality) and Art. 1 (human dignity).

112 Stefano Rodotà, *Data Protection as Fundamental Right*, p 2.

113 Julie E. Cohen, 126. *HLR* 2013, p 1906.

114 Julie E. Cohen, 126. *HLR* 2013, p 1908.

115 Elettra Bietti, *The Discourse of Control and Consent over Data in EU Data Protection Law and Beyond*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper

approach simply shifts the regulatory burden onto the consumers, who, as we have argued, are not sufficiently aware of the details of data collection and processing, and are vulnerable to interface design manipulation.[116] This serves the interests of the industry, as they are free to engage in new forms of data processing, staying one step ahead the regulator, provided they obtain consent of the users, which could be as simple as having them tick a box[117] (though not 'unticking' a pre-ticked box).[118]

In other words, the regulatory response, which relies solely on ensuring a negative freedom (i.e., lack of pressure, undue influence, coercion) to give consent, is inapposite where consumers are not in a position to give informed consent in the first place.

46. A possible response to this criticism may be that these provisions are meant to strike an equilibrium between protecting the citizens' rights and at the same time facilitating business.[119] Bietti's retort is that conceptualizing privacy as informational self-determination, which demonstrates itself in the current regulatory reliance on the notion of consent, premises on 'faith in individuals as the ultimate and best decision makers'.

Yet, it is not apparent that such faith is warranted. Even assuming that the current balance struck by the EU regulatory regime between the autonomy of individual consumer and the needs of commercial actors is satisfactory, it ignores a vital technological reality of Big Data. Large-scale data collection and the predictive algorithmic processing thereof, allow one individual's data to inform decisions regarding another's. In this sense, the decision of one individual spills over to affect the decisions of others, often in varying degrees of significance. For example, A's decision to allow access to data regarding their shopping habits may, after an opaque data-processing method, result in B being denied access to a loan. In this regard an approach that focuses on the personal and discrete decisions of one individual, without regard to the broader context and uses of the technology are flawed.

More pragmatically however, the belief in the rugged individualism and autonomy of EU consumers seems to be naïve for the very simple reason that the technological process itself is opaque and constantly changing.[120] Hence, the idea that an individual would be in a place to give 'fully informed consent' is unjustified

---

2020, No 2001, https://www.lawfareblog.com/discourse-control-and-consent-over-EU-data-protection-law-andbeyond (accessed 9 March 2020), pt 1.

116 Elettra Bietti, *The Discourse of Control*, p 1.

117 GDPR, Recital 32.

118 ECJ 1 Oct. 2019, *supra* n. 57, *Planet49*, p 63.

119 DCD, Recital 2; Inge Graef, Thomas Tombal & Alexandre Steel, *Limits and Enablers of Data Sharing: An Analytical Framework for EU Competition, Data Protection and Consumer Law*, DP 2019-024 TILEC Discussion Paper (2019), p (1) at 11.

120 Elettra Bietti, *The Discourse of Control*, p 5.

absent a method to ensure that the consumer is actually in a place to understand and appreciate how and why their data is being used.

47. On the other hand, it is difficult to see what better organizing concept could be devised that is preferable to that of 'consent'. Perhaps the best way forward is not in abandoning the notion of concept altogether, especially as various areas of EU law were constructed with it firmly baked into their core, but rather to strive for increasing the level of awareness of consumers. We should aim to make sure that the consumers (rather than our *ex-ante* regulation, which borders the impossible) keep up with the pace of the technological development.

4.2 Discrimination

48. Next let us scrutinize how EU law attempts to address the issue of Big-Data-related prejudicial discrimination. Under the GDPR, processing of 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership' is prohibited.[121] Furthermore, the Regulation provides the data subjects with a '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'.[122] However, both these rights are subject to exceptions, and both do not apply if such data processing is consented to by the individual.[123] Here, we can directly refer to the critique of the centrality of consent that we presented above.

49. Additionally, the prohibition of processing data '*revealing*' the protected characteristics does not apply if it 'relates to personal data which are manifestly made public by the data subject'.[124] This means that indirect discrimination by algorithmic decision-making can still take place. For example, if the algorithm links some names, place of residence, interests etc. to race (as has been the case)[125] and on that basis determines that the risk level is higher and so it should be reflected in price (individual price discrimination) or contract should be refused all together.

This conduct would be lawful under the GDPR, provided the algorithm received such information from, say, a social media profile of the consumer ('manifestly public' by definition). The current Consumer Protection regime does not do enough to make sure that indirect discrimination on the basis of protected characteristics (race, gender, religion, sexual orientation etc.), does not take place in the world of highly commercialized personal data.

---

121 GDPR, Art. 9(1).
122 GDPR, Art. 22(1).
123 GDPR, Arts 9(2)(a), 22(2)(c).
124 GDPR, Art. 9(2)(e).
125 See above s. 3.3.

4.3 Commission's Response

50. The Commission in their New Deal for Consumers tried to address some of the perceived inadequacies in the Consumer *acquis* exposed by the Big Data revolution risks. We argue that their response fell short in addressing the lacuna created by the mass-scale commercialization of personal data, as well as failed to address some of the risks we outlined above altogether.

51. Directive 2019/2161 amended the 'CRD', to include a provision mandating disclosure by the trader to the consumer where 'the price was personalized on the basis of automated decision-making'.[126] This fails to address the problem fully.

This inclusion seems to legitimize individualized price discrimination as an acceptable commercial practice.[127] Recital 45 of the 2019 Directive expands on this point explaining that 'this information requirement should not apply to techniques such as "dynamic" or "real-time" pricing that involve changing the price in a highly flexible and quick manner in response to market demands' but only to pricing decisions made on the basis of 'automated decision-making and profiling of consumer behaviour allowing traders to assess the consumer's purchasing power'.-[128] This explicitly permits (provided Article 6(1) CRD is observed) traders to 'profile' users and adjust their prices accordingly. The flaw contained in this provision is not remedied by the statement that it is 'without prejudice' to the GDPR provisions, given the inadequacy of the Regulation to prevent discrimination outlined above.

52. Prior to the 2018–2019 legislative push, which enacted the New Deal for Consumers, EU consumer law was simply inadequate, relying on out-dated framework of political values and regulatory measures, especially as regards the ability to accommodate the increasingly digitized consumer markets.[129]

Crucially, the CRD was simply ill designed to deal with the reality where personal data was exchanged for goods and services. Prior to the New Deal for Consumers, the CRD used to define a 'sales contract' as a contract where 'the trader transfers or undertakes to transfer the ownership of goods [or services] to the consumer and the consumer pays or undertakes to pay the *price* thereof'[130]; where '*price*' was later defined as '*money* or a digital representation of value that is due in exchange for the supply of digital content or a digital service'.[131]

---

126 Dir 2019/2161, Art. 4(4)(a)(ii) inserting Art. 6(1)(ea) into the CRD.

127 Melvin Tjon Akon, *Personalized Pricing Using Payment Data: Legality and Limits under European Union and Luxembourg law* (1 December 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536187 (accessed 27 Febuary 2020), p (1) at 13–14.

128 Dir 2019/2161, Recital 45.

129 Mateusz Grochowski, 39. *Yearbook of European Law* 2020, pp 388–389.

130 CRD, Art. 2(5).

131 DCD, Art. 2(7).

Accordingly, prior to the New Deal, there were at best weak and indirect methods to update the EU Consumer Protection regime. First, the personal data provided in exchange for a service could have been understood as a 'digital representation of value', to fit data in the pre-existing definition of 'price', and thus bring instances of commercialization of consumers' personal data within the existing regime.

Second, the notion of 'obligation to pay' could have been expanded to include instances where personal data is exchanged for goods or services. The CRD did (and continues to) require the trader to 'ensure' that the consumer 'explicitly acknowledges that the order implies an obligation to pay'.[132] Thus it appeared possible to 'update' the CRD to accord with the demands of the Big Data world by interpreting this provision as requiring traders to inform their consumers where their personal data is collected and monetized for value, in exchange for access to a good or a service. However, this would have been a very indirect and tenuous method of adapting the EU Consumer *acquis* to the Big Data reality, and in any event no such interpretation of Article 8(2) CRD was advanced by the CJEU.

Thirdly, the notion of 'commercial practices' under UCPD,[133] which is sufficiently broad, could have been interpreted to apply to the commercialization of consumer's data. Since it was already considered an 'unfair practice' to label a service as 'free of charge' when it was not,[134] this provision could have been extended to apply to instances where consumers unknowingly exchanged their personal data for supposedly free digital services.

Lastly, even before the New Deal for Consumers was adopted, the provisions of the Unfair Contract Terms Directive (UCTD) applied to all consumer contracts, with the effect that terms of a consumer contract could not 'contrary to the requirement of good faith ... cause a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer'.[135]

Yet, under the UCTD the assessment of the unfairness could not be conducted on terms relating to the 'definition of the main subject matter of the contract nor to the adequacy of the price and remuneration'.[136] If personal data was understood as 'price' or 'digital representation of value' as postulated by the Digital Services Directive (DSD) and the CRD, then this seemed to have excluded the application of the UCTD to instances of monetization of consumers' personal data by traders.

In short, prior to the New Deal, the UCTD and the UCPD did not expressly limit or police the occasions where personal data of consumers could be collected and commercialized by traders, but rather insisted on the balance, fairness and

132 CRD, Art. 8(2).
133 CRD, Art. 2(d).
134 Unfair Commercial Practices Directive, Annex I, para. 20.
135 Unfair Contract Terms Directive, Art. 3(1).
136 Unfair Contract Terms Directive, Art. 4(2).

transparency in consumer-trader contractual relations.[137] This was inadequate in the Big Data context, and it was opined that 'the existing Union consumer protection rules should be modernised'.[138]

53. This perceived inadequacy of the old regime was addressed in a string of legislative measures passed by the Commission. Firstly, Directive 2019/2161 amended the CRD and changed the definition of 'sales contract': now it is defined as 'any contract under which the trader transfers or undertakes to transfer ownership of goods to the consumer',[139] removing the problematic (in the personal data context) reference to 'price' or 'digital representation of value'.

The Digital Content Directive, as well as the Directive 2019/2161, now expressly apply also 'where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader'.[140] This clear and unambiguous extension of the Consumer Protection regime to instances of commercialization of personal data is welcome, and removes any uncertainty and artificiality in attempting to extend the old regime by creative interpretation.

Directive 2019/2161, further adds to the UCPD by providing that information as to whether the seller is a 'trader' or not, on the online marketplace, is to be 'material' for the purposes of determining if its omission is 'misleading' under Article 7 UCPD.[141] Furthermore, the Directive raises penalty ceilings, in an attempt to ensure better enforcement of consumer rights and improved deterrent effect against breaching consumer law obligations[142]: under the new rules, the competent authorities may introduce penalties equivalent to 4% of annual turnover or where turnover is not ascertainable, 2 million Euros.[143]

54. Lastly, we should analyse the new right of data portability, enshrined in the GDPR[144] and the DCD.[145] This right is another step in bolstering the individual's right to self-management and consumer autonomy, by allowing the data subject to move their personal data from one controller to another.[146] The two regimes are complimentary, which further shows the co-operation of the various fields of EU law that have to interact to safeguard the protection of consumer rights.

---

137 Inge Graef, Thomas Tombal & Alexandre Steel*Limits and Enablers of Data Sharing*, p 13.
138 DCD, Recital 17.
139 Dir 2019/2161, Art. 4(1)(c).
140 DCD, Art. 3(1); Dir 2019/2161, Art. 4(2)(b); CRD, 3(1a).
141 Dir 2019/2161, Art. 3(4)(a)(ii).
142 Dir 2019/2161, Recitals 14 and 16.
143 Dir 2019/2161, Arts 1(4) (5), 3(6) and 4(13).
144 GDPR, Art. 20.
145 DCD, Art. 16.
146 Inge Graef, Thomas Tombal & Alexandre Steel, *Limits and Enablers of Data Sharing*, pp 13, 18.

55. Under the GDPR, the data subject has a 'right to receive the personal data concerning him or her, which *he or she has provided* to a controller',[147] where the processing is based on consent, or is necessary for the performance of the contract.[148] This is not a general right to data portability, because it does not apply to data processing which occurs in compliance with a legal obligation to which the data controller is subject,[149] or where the data is one generated by the controller rather than supplied by the consumer.

The Working Party has defined 'provided' as 'data *actively and knowingly* provided by the data subject' (name, age, email address, etc.) and 'observed data provided by the data subject by virtue of the use of the service or the device' (search history, traffic and localization data, etc.).[150] Such a characterization still leaves out data pertaining to identifiable consumers (hence 'personal data' under GDPR) that is not covered by the right to portability enshrined in Article 20. Predictive algorithmic analytics will have the capability to turn supposedly neutral data (such as IP address) that would be so 'provided' into identifiable data that would not, meaning the latter would be out of reach of the consumer.

56. The Digital Content Directive requires traders 'at the request of the consumer, [to] make available to the consumer any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader'.[151] The same right was added to the CRD by Directive 2019/2161.[152]

These provisions thus introduce a right to portability of *non*-personal data, since that would qualify as 'any content other than personal data'. They do not allow the direct transmission of data between two traders, contrary to the GDPR,[153] but still the underlying idea is to promote the autonomy of consumers and thus remedy the imbalance between the traders and consumers while promoting a vibrant data market.[154]

57. However, the data-portability solution borrowed by the Consumer Protection regime from the GDPR may be problematic because it incorporates the distinction between 'personal' and 'non-personal' data.

---

147 GDPR, Art. 20(1) (emphasis supplied).
148 GDPR, Art. 20(1).
149 GDPR, Art. 20(3).
150 Working Party 29, *Guidelines on the Right to Data Portability* (2017), WP 242 rev.01, pp 8-9.
151 GDPR, Art. 16(4) (in the event of termination).
152 Dir 2019/2161, Art. 4(10); CRD, Art. 13(4)-(7) (as amended).
153 GDPR, Art. 20(1) and (3).
154 Inge Graef, Thomas Tombal & Alexandre Steel, *Limits and Enablers of Data Sharing*, p 18.

58. 'Non-personal' data is understood in EU law to mean 'electronic data other than personal data as defined in Article 4(1) GDPR'.[155] A negative definition ('other than personal data ...') seems to presuppose that the meaning of 'personal data' is clear-cut; on the contrary however, it seems that the definition adopted in the GDPR is not settled at all, and remains uncertain.[156]

The problem with this delineation is compounded by the Big Data revolution, which rapidly expands the field of 'information relating to an identified or identifiable natural person'.[157] Consequently, data which is initially seen as non-personal may by virtue of more advanced analytics become personal later down the line which would create problems in practice.[158] Hence even this method of strengthening the autonomy of consumers is inadequate to deal with the increasing commercialization of consumer data.

59. To summarize our argument is that consumer law is unable to keep with the ever-developing field of Big Data, which means that it alone is insufficient to safeguard the fundamental rights of consumers, and needs to be supported by other fields of EU law, such as competition law and data protection law. The GDPR signals precisely this new dawn of interdisciplinary approach.

5. Interdisciplinary Approach

60. EU competition, data protection and consumer law seem to be sharing the same purpose, at least to some extent. They all attempt to achieve 'the integration of the internal market' and to 'protect the welfare of consumers or data subjects'.[159] At the same time, the means by which this shared objective is pursued differ between the three disciplines: Competition Law intervenes against abuse of monopolist behaviour, Consumer Law addresses the imbalance of bargaining power between consumer and trader, whereas data protection law grants data subjects control over their personal data.[160]

Perhaps then, it is in the merging of the three's means that we can address the momentous challenge posed by the big data revolution. The EDPS

155 Regulation 2018/1807 of 14 Nov. 2018 on a framework for the free flow of non-personal data in the European Union, http://data.europa.eu/eli/reg/2018/1807/oj, Art. 2(1).

156 Inge Graef, Raphaël Gellert & Martin Husovec, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data Is Counterproductive to Data Innovation', 44. *European Law Review* 2019, p (605) at 608.

157 'Personal data' as defined in GDPR, Art. 4(1).

158 Inge Graef, Thomas Tombal & Alexandre Steel, *Limits and Enablers of Data Sharing*, p 12.

159 Inge Graef, Thomas Tombal & Alexandre Steel, *Limits and Enablers of Data Sharing*, p 3.

160 Inge Graef, Thomas Tombal & Alexandre Steel, *Limits and Enablers of Data Sharing*, p 4.

has already called for a 'more holistic approach to enforcement' of EU laws on data protection, consumer protection and competition.[161]

61. To begin with, in light of the issues with consumer consent outlined above it might be beneficial to supplement the consent test with the fairness test prominent in consumer protection law, and enshrined in Directive 1993/13 on unfair contracts terms (UCTD). In fact, there is some cross-pollination between the language used in the UCTD and GDPR in terms of introducing a notion of fairness.[162] Fairness plays a pivotal role in consumer protection law, as the standard, which is used to determine the legality of contract terms and commercial practices.[163] Consumer law might be an extra safeguard to ensure that the conditions under which consumers part with their personal data are not unfair; conversely, data protection law might be useful in assessing the fairness of a consumer contract – a contract might create a significant imbalance in the rights and obligations of the parties, to the detriment of the consumer, against the requirement of good faith, if it breaches the data protection law's requirements.[164] In fact the EDPS has added a principle of 'fairness' to the list of core principles (amongst the principles of lawfulness and transparency) of data protection.[165] These can be supported by Articles 101 and 102 Treaty on the Functioning of the European Union (TFEU) which would prevent sharing data in situations where it could give rise to collusion that could not be justified under Article 101(3) TFEU,[166] curbing the abuse of dominant position by the data behemoths.

62. Additionally, consumer law may be very useful in terms of providing concrete rights to consumers if the data protection obligations are violated. Under the current data protection regime, the consequence of breach is that data processing becomes unlawful, but the mere presence of unlawfulness of data processing does not say a lot about the consequence for a possible

---

161 Arno Scharf, 'Exploitative Business Terms in the Era of Big Data – the Bundeskartellamt's Facebook Decision', 40. *European Competition Law Review* 2019, p (332) at 333.

162 Compare GDPR, Recital 43: 'In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller ... ' and Unfair Contract Terms Directive, Art. 3(1): A contractual term (...) 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'.

163 Inge Graef, Damian Clifford & Peggy Valcke, 8. *IDPL* 2018, p 204.

164 Natali Helberger, Frederik Zuiderveen Borgesius & Agustin Reyna, 'The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law', 54. *Common Market Law Review* 2017, p (1427) at 1451.

165 Inge Graef, Damian Clifford & Peggy Valcke, 8. *IDPL* 2018, p 203.

166 Inge Graef, Thomas Tombal & Alexandre Steel, *Limits and Enablers of Data Sharing*, p 6.

contractual relationship between trader and consumer.[167] Consumer protection law can be thus used to bolster the data protection measures provided for in the GDPR for example.[168]

63. Perhaps due to the different means that the two disciplines adopt in pursuit of the objective they continue to operate on the basis of different principles: data protection's main principles are lawfulness, transparency, purpose limitation and data minimization; conversely consumer law is less 'clearly linked to the protection of a fundamental right' and aims to 'set the basic rules for the bargaining game' thus drawing most heavily from the principles of fairness and protection.[169] The main objectives of consumer law seems to be to empower the consumers as a sovereign market actor, and to protect them when they are in a weaker bargaining position.[170] The first limb of that however does not seem to be that distant from the approach taken by the GDPR, which hints that the Regulation blurs the not-so-bright line between the two areas of law. In that context, the conclusion that data protection and consumer laws share, at least to an extent, the same purposes seem to be evident. Helberger et al. argue that both disciplines are united by their use of information as a 'means to mitigate information asymmetries and to empower the individual'.[171]

64. Pragmatically however, it does remain the case that the two areas of law remain 'two different fields, with different legal traditions, concepts and objectives'.[172] However, as follows from the preceding analysis, the differences are not insurmountable and some steps have already been taken that assimilate data protection law and consumer protection law, making the two disciplines ever more united. This unification on principles is a prerequisite for an effective safeguard of consumers in the era of mass commercialization of consumers' personal data. Big Data poses a big challenge that can best be met by a coordinated response, and while at the conceptual level there may be some differences between consumer protection law and data protection law, such differences are far from insurmountable. At the enforcement level, the need for harmonization between those disciplines is significant.

6. Conclusions

65. It has been argued that the increased commercialization of consumer data poses serious threats that challenge the traditional approach of consumer

167 Natali Helberger, Frederik Zuiderveen Borgesius & Agustin Reyna, 54. *CMLR* 2017, p 1440.
168 Inge Graef, Damian Clifford & Peggy Valcke, 8. *IDPL* 2018, p 206.
169 Natali Helberger, Frederik Zuiderveen Borgesius & Agustin Reyna, 54. *CMLR* 2017, p 1437.
170 Natali Helberger, Frederik Zuiderveen Borgesius & Agustin Reyna, 54. *CMLR* 2017, p 1437.
171 Natali Helberger, Frederik Zuiderveen Borgesius & Agustin Reyna, 54. *CMLR* 2017, p 1437.
172 Natali Helberger, Frederik Zuiderveen Borgesius & Agustin Reyna, 54. *CMLR* 2017, p 1460.

protection law. Consequently, if the EU is serious about its commitment to the high level of consumer protection it must address the shortcomings of the existing legal regime. We have illustrated that the Cambridge Analytica scandal is only a front-page example of how the commercialization of consumer data should increasingly move to the top of the legislative and regulatory agenda.

66. Consumer law has not said its last word regarding the commercialization of consumer data – it is suggested that building on the basic rights prescribed for consumers (in their capacity as data subjects) by the GDPR, EU consumer law can provide more effective remedies, and extend the traditional consumer protection to areas of supply of digital services and content. What is needed is a switch from chasing the technology as it develops, to focusing on creating a contracting landscape where the consumer may be properly informed in material respects, and the regulator vigilant where such level of awareness is impossible. To that end, the current approach of the EU is one step forward in the right direction, but which still falls short.

67. Equally, we have shown that there is a serious difficulty with the law keeping up with technological development of Big Data. That is why the EU response to the problem, through the recent Directive 2019/2161 on modernization and better enforcement of EU consumer law, was a step in the right direction, though it still had problems, namely the blurred bifurcation between personal and non-personal data, the continued reliance on consumer consent, despite the indications of the inability of data processors and controllers to faithfully rely on the consent, and the continued commitment to the autonomy paradigm as a panacea to any potentially exploitative commercial practice. Further, the issue of indirect discrimination remains unaddressed.

68. The answer to this great challenge will lie in some form of united answer of competition, consumer protection and data protection laws, and it would be naïve to expect traditional norms of consumer *acquis* to provide the exhaustive response. Nonetheless, given the pace of the advancement it is suggested that the awareness of the consumers must be continued to be expanded because therein lies the one true condition for the success of the autonomy paradigm in the protection of personal data.

69. It is apt to conclude with a quote from the Cambridge Analytica whistle-blower, illustrating the reality of the consequences of mass commercialization of consumer personal data: 'the only morality of the algorithm is to optimize you as a consumer ... you become the product'.[173]

---

173 Kate Magee, *Cambridge Analytica Whistleblower Christopher Wylie: It's Time to Save Creativity*, Campaign (5 November 2018), https://www.campaignlive.co.uk/article/cambridge-analytica-whistleblower-christopher-wylie-its-time-save-creativity/1497702 (accessed 9 March 2020).

This work was supported by PANELFIT, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039.

This article was first published in the EUROPEAN REVIEW OF PRIVATE LAW (Vol.29, Nr.5-2021, [701 – 732], 2021 © Kluwer Law International BV, The Netherlands).