Common Market Law Review **57**: 1461–1494, 2020.

KALEIDOSCOPIC DATA-RELATED ENFORCEMENT IN THE DIGITAL AGE

SVETLANA YAKOVLEVA, WESSEL GEURSEN AND AXEL ARNBAK*

Abstract

The interplay between competition, consumer and data protection law, when applied to data collection and processing practices, may lead to situations where several competent authorities can, independently, carry out enforcement actions against the same practice, or where an authority competent to carry out enforcement in one area of law can borrow the concepts of another area to advance its own goals. The authors call this "kaleidoscopic enforcement". Kaleidoscopic enforcement may undermine existing coordination mechanisms within specific areas, and may lead to both the incoherent enforcement of EU rules applicable to data, and to sub-optimal enforcement. An EU level binding inter-disciplinary coordination mechanism between competition, consumer and data protection authorities is needed. Now the Commission has announced ambitious plans to enhance the coherent application of EU law in several areas, it is the perfect time to work towards creating such an enforcement mechanism.

* Svetlana Yakovleva is a senior legal adviser in Privacy and Cybersecurity at De Brauw Blackstone Westbroek and PhD candidate at the Institute for Information Law (IViR), University of Amsterdam. Wessel Geursen is a senior legal adviser in EU & Competition law at De Brauw Blackstone Westbroek and affiliated PhD fellow at the Vrije Universiteit. Axel Arnbak is a lawyer at De Brauw Blackstone Westbroek and research fellow at the Institute for Information Law (IViR), University of Amsterdam. The authors would like to thank Harm-Jan de Kluiver and the participants of the workshop on the earlier version of this article at the Privacy Law Scholars Conference Europe (PLSC-E) 2019, Amsterdam, the Netherlands, and specifically Inge Graef, for their careful reading of the article and insightful comments and suggestions. The authors are also grateful to Daan Hereijgers, Stephen Jones and Leticia Vasquez for their assistance with preparation of this article for publication. All errors are authors' own. The views expressed in this article are personal views of the authors and do not represent a position of De Brauw Blackstone Westbroek.

A different and less developed version of our research and thoughts on kaleidoscopic enforcement was published in Dutch: "Caleidoscopische handhaving tegen het datagebruik van ondernemingen" in Moerel et al. (Eds.), *Vereeniging "Handelsrecht" Preadviezen 2019 – Onderneming, digitalisering en data – Over corporate governance en handhaving in het digitale tijdperk* (Uitgeverij Paris, 2019), p. 57.

1. Introduction

Ten years ago, Meglena Kuneva, European Commissioner for Consumer Protection, said that "personal data is the new oil of the internet and the new currency of the digital world".[1] Although incorrect in some respects,[2] this metaphor is telling. Ten years later, we see that the access to and the ability to monetize personal and other data has indeed become an essential factor in being able to compete in the digital economy. The oil and gas industries have given way to the technology industry, as the latter begins to dominate the world's top 20 companies by market capitalization.[3]

We start from the basic assumption that data is crucial not only to gain a competitive edge, but also to survive in the digital economy and to gain (geo)political power, and that access to and the use of data will continue to be key to commercial success in the years to come, in every sector imaginable.[4] The decisive element to success in the digital age is not limited to the amount of investment in research and development of hardware or complex technologies, such as artificial intelligence (AI) and machine learning. Massive troves of accurate data are needed to train algorithms and other automated decision-makers that underlie our envisioned age of big data, advanced analytics, and artificial intelligence. That is why medical institutions in the Netherlands sounded the alarm in the Dutch press about strict EU privacy and data protection rules: while the latter restrict full-blown access to and the use and re-use of patient data, Chinese and American research laboratories and companies are winning the race in the next generation of medical solutions.[5]

1. See Kuneva, "Keynote Speech – Roundtable on online data collection, targeting and profiling", Brussels, 31 March 2009, <europa.eu/rapid/press-release_SPEECH-09-156_en.htm>, (all websites last visited 29 July 2020). See also "The world's most valuable resource is no longer oil, but data", *The Economist*, 6 May 2017 <www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

2. Forbes, "Here's why data is not the new oil", 5 March 2018, <www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/>.

3. While in 2009, companies in the oil and gas sector accounted for 36% of market capitalization, by 2018, technology and consumer services accounted for 56% of market capitalization, whereas the share of oil and gas companies had dropped to just 7%. See UNCTAD Digital Economy Report 2019, 4 Sept. 2019 (UNCTAD/DER/2019), p. 17.

4. See "China and US compete to dominate big data", *Financial Times*, 1 May 2018, <www.ft.com/content/e33a6994-447e-11e8-93cf-67ac3a6482fd>.

5. See "Strenge privacyregels hinderen medisch onderzoek in Nederland", *Het Financiële Dagblad*, 23 Sept. 2019, <fd.nl/ondernemen/1316827/strenge-privacyregels-hinderen-medisch-onderzoek-in-nederland>.

Similarly, as data is "the raw material for AI", access to it for re-use is indispensable in order to succeed in the global race for AI dominance.[6] Online platforms further build on this point. Recently, competition, consumer and data protection authorities across Europe investigated Facebook, Google, Amazon and other platforms for their harvesting and monetization of user data.[7] One of the key commercial success factors here is whether a market player succeeds in reaching near-monopoly status due to network effects.[8] These market players make platforms more valuable to particular users (both consumers and sellers on the platforms alike) if most other users are also present on such platforms, but they also allow the collection of more user data and use of insights from processing that data to further improve their services.[9] Indeed, Facebook only truly realized social network hegemony in

6. Commission Communication, "Artificial Intelligence for Europe", COM(2018)237 final, at p. 3; Forbes, "Why the race for AI dominance is more global than you think", 9 Feb. 2020, <www.forbes.com/sites/cognitiveworld/2020/02/09/why-the-race-for-ai-dominance-is-more-global-than-you-think/#1eab9ae7121f>; Commission Communication, "A European strategy for data", COM(2020)66 final, at p. 2; Commission, White Paper on Artificial Intelligence. A European approach to excellence and trust, COM(2020)65 final, at p. 1.

7. See e.g. *Bundeskartellamt* decision 6 Feb. 2019, Case B6-22/16, *Facebook*; CMA, "Online platforms and digital advertising market study", 3 July 2019, <www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study>; Hirst, "Facebook prompts EU antitrust questions over data, marketplace", 2 July 2019, <mlexmarketinsight.com/insights-center/editors-picks/antitrust/europe/facebook-prompts-eu-antitrust-questions-over-data-marketplace>; "Key findings of the Italian joint sector inquiry into big data", *Media Laws*, 18 March 2020, <www.medialaws.eu/key-findings-of-the-italian-joint-sector-inquiry-into-big-data/>; European Commission, "Antitrust: Commission opens investigation into possible anti-competitive conduct of Amazon", 17 July 2019, <ec.europa.eu/commission/presscorner/detail/en/IP_19_4291>; European Commission, "Booking.com commits to align practices presenting offers and prices with EU law following EU action", 20 Dec. 2019, <ec.europa.eu/commission/presscorner/detail/en/ip_19_6812>; "EU to investigate Google over data collection practices", *The Guardian*, 2 Dec. 2019, <www.theguardian.com/technology/2019/dec/02/eu-investigates-google-data-collection-practices>; Autoriteit Persoonsgegevens, "Dutch data protection authority: Facebook violates privacy law", 16 May 2017, <autoriteitpersoonsgegevens.nl/en/news/dutch-data-protection-authority-facebook-violates-privacy-law>; CNIL, "The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC", 21 Jan. 2019, <www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>.

8. Shapiro and Varian, *Information Rules: A Strategic Guide to the Network Economy* (Harvard Business School Press,1999), pp. 13–14 and 183–184.

9. COM(2020)66 final, cited *supra* note 6.

the West after acquiring WhatsApp and Instagram.[10] Although these near-monopolies may create benefits for the users (consumers and small and medium enterprises (SMEs) that use these platforms to offer their services), as platforms gain market power, they can use it to the detriment of both their users and competitors. They do this by restricting competition, both in the market for the services *of* the platforms and in the market for goods and services provided *on* the platform.[11] This "winner-takes-(almost)-all" effect is caused by the number of users on their platforms and, perhaps predominantly, by the massive troves of personal data they have about their users.[12]

Similarly, as (personal) data has become a factor of production of goods and services and a form of remuneration for "free" services on two-sided markets (such as social media platforms),[13] companies generate a variety of insights about consumers by using various data processing technologies, including machine learning and artificial intelligence. This exacerbates the asymmetry of information between companies and consumers and may allow the former to exploit consumers' behavioural biases, undermine consumers' choices and discriminate.[14]

The cross-cutting nature of data in the digital economy has prompted a new twist in the relationship between data protection, competition and consumer law, which manifests itself in both the convergence of these legal domains and in new points of tension between them. These are described in the growing volume of literature and regulatory guidance and policy documents.[15]

10. According to Taha Yasseri, a senior research fellow at the Oxford Internet Institute, "One company owning four of the most popular social networking and communication apps, at best, can be described as a data monopoly." BBC News, "Facebook owns the four most downloaded apps of the decade", 18 Dec. 2019, <www.bbc.com/news/technology-50838013>.

11. COM(2020) 66 final, cited *supra* note 6, p. 8.

12. Gökçe Dessemond, "Restoring competition in 'winner-took-all' digital platform markets", Dec. 2019 *UNCTAD Research Paper* no. 40. As the European Commission has phrased it: "strong indirect network effects that can be fuelled by data-driven advantages by the online platforms". See Explanatory memorandum to the proposal by the European Commission for a regulation on promoting fairness and transparency for business users of online intermediation services, COM(2018)238 final.

13. See e.g. Bataineha et al. "Monetizing personal data: A two-sided market approach", 83 *Procedia Computer Science* (2016), 472.

14. See e.g. Calo, "Digital market manipulation", 82 *George Washington Law Review* (2014), 995–1051, at 1003.

15. See e.g. Robertson, "Excessive data collection: Privacy considerations and abuse of dominance in the era of big data", 57 CML Rev. (2020), 161–190, at 186–187; Helberger, Zuiderveen Borgesius and Reyna, "The perfect match? A closer look at the relationship between EU consumer law and data protection law", 54 CML Rev. (2017), 1427–1466; Costa-Cabral and Lynskey, "Family ties: The intersection between data protection and competition in EU law", 54 CML Rev. (2017); Graef, Clifford and Valcke, "Fairness and enforcement: Bridging competition, data protection, and consumer law", 8 *International Data Privacy Law* (2018); Graef, "Blurring boundaries of consumer welfare. How to create

Looking at the interaction between substantive competition, consumer, and data protection rules from an *enforcement angle*, this article demonstrates how such interaction leads to what we call "kaleidoscopic enforcement".[16] This occurs when: (i) more than one of the authorities has a legal basis and competence to initiate an enforcement action against the same data processing practice (parallel enforcement actions);[17] or (ii) an enforcement authority borrows the concepts of one area of law to interpret the rules of the area of law it is empowered to enforce to achieve the goals of this latter area of law (internalization of the rules of one area of law to further the goals of the other).[18] Until now, parallel enforcement has only happened between different EU Member States.[19] However, as this article shows, there are no legal barriers to parallel enforcement within one and the same EU Member State.[20] The problem of kaleidoscopic enforcement is compounded when competition, consumer, and data protection rules are enforced through private parties instead of, or in addition to, public enforcement.[21] Both the discussion in this

synergies between competition, consumer and data protection law in digital markets" in Bakhoum et al. (Eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach?* (Springer, 2018); Botta and Wiedemann, "The interaction of EU competition, consumer, and data protection law in the digital economy: The regulatory dilemma in the *Facebook* odyssey", 64 *The Antitrust Bulletin* (2019); EDPS Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, 23 Sept. 2018; Crémer, De Montjoye and Schweitzer, *Competition Policy for the Digital Era* (Publications Office of the EU, 2019).

16. Other authors call it "regulatory dilemma". See Botta and Wiedemann, op. cit. *supra* note 15. With regard to public-private enforcement of competition law alone, Jones uses the term "enforcement pluralism", which could in our view also be used with respect to public enforcement by various authorities. C.A. Jones, *Private Enforcement of Antitrust Law in the EU, UK and USA* (OUP, 1999), p. 85.

17. For discussion, see *infra* section 2.2.

18. For discussion, see *infra* section 2.3.

19. For an overview see e.g. Carugati, "The 2017 Facebook saga: A competition, consumer and data protection story", 2 *European Competition and Regulatory Law Review* (2018), 4–10.

20. For discussion, see *infra* section 3.3.

21. In respect of consumer law, a shift can been seen to private enforcement through collective actions; cf. Scott, "Consumer law, enforcement and the new deal for consumers", (2019) E.R.P.L., 1279–1296. Germany and Austria are the only two Member States where private enforcement was already the main instrument of enforcement of consumer law, although the German *Bundeskartellamt* has been entitled to conclude that there has been an infringement since 2017; cf. Podszun, Busch and Henning-Bodewig, "Consumer law in Germany: A shift to public enforcement?", (2019) *Journal of European Consumer and Market Law*, 75–82. With regard to private enforcement of competition law, Hjelmeng concludes that "[a]s regards implementation of private enforcement in Europe, there are challenges pertaining to the lack of a coherent regulation on an EU level, the limited use of private enforcement, and 'enforcement pluralism' and coordination between the different courts and agencies involved", Hjelmeng, "Competition law remedies: Striving for coherence or finding new ways?", (2013) CML Rev., 1007–1037, at 1035. With regard to private enforcement of data protection law, see Pato, "The collective private enforcement of data protection rights in the EU", <dx.doi.org/10.2139/ssrn.3303228>.

article and the proposed solution to kaleidoscopic enforcement, however, look solely at public enforcement.

Although kaleidoscopic enforcement could be viewed as beneficial – in that it allows the three respective areas of law to reinforce each other – it has significant drawbacks, which need to be addressed. These drawbacks include: the inconsistent interpretation of data protection rules by competition, consumer, and data protection authorities, resulting in legal uncertainty as to the meaning of those rules; the disruption of existing coordination mechanisms within each respective area of law; the under-enforcement or over-enforcement of rules on data collection and use; and employing practices detrimental to the goals of one or several respective areas of law.[22] We expect that these drawbacks will only be exacerbated in the future: the strategic agendas of various supervisory authorities show that enforcement against companies' activities involving the collection and use of personal and other data will intensify in the next few years.[23]

To properly address the negative implications of kaleidoscopic enforcement in the digital age, we argue, a coherent multidisciplinary approach is

22. See *infra* section 3.

23. It is inherent in DPAs' competence to enforce in relation to the use of personal data. Competition and consumer authorities enforce rules against data-related practices under the auspices of regulating the digital economy. Crémer, De Montjoye and Schweitzer, op. cit. *supra* note 15; European Commission, "Press remarks by President von der Leyen on the Commission's new strategy: Shaping Europe's digital future", 19 Feb. 2020, <ec.europa.eu/commission/presscorner/detail/en/speech_20_294>; Mission letter of Ursula von der Leyen, President-elect of the European Commission, to Didier Reynder, Commissioner Designate for Justice, 10 Sept. 2019, <ec.europa.eu/commission/presscorner/detail/en/speech_20_294>; See also Micklitz, "Consumer law in the digital economy" in Kono, Hiscock and Reich (Eds.), *Transnational Commercial and Consumer Law: Current Trends in International Business Law Perspectives in Law, Business and Innovation* (Springer, 2018), pp. 111–152; Dutch Authority for Consumers and Markets, "Missie en Strategie", <www.acm.nl/nl/organisatie/missie-en-strategie/onze-agenda/acm-agenda-2020-2021/digitale-economie> (stating that in 2020–2021 the ACM will focus on online deception and access to platforms and ecosystems. The European Data Protection Board (EDPB) has recently warned the Commission of the potential negative effects of market concentration, especially in the technology sector of the economy, on data protection and consumer rights, at the time of the proposed acquisition of Shazam by Apple. The EDPB urged the Commission to assess long-term implications of such mergers on the fundamental rights to privacy and personal data, and indicated that DPAs can help with the assessment of those implications, see <edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_en.pdf>; EDPB, Statement on privacy implications of mergers, 19 Feb. 2020, <edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_privacyimplicationsofmergers_en.pdf>.

necessary, not only in terms of substantive rules[24] but also, and most importantly, at the *institutional level*. Given the different goals pursued by competition, consumer, and data protection authorities, the silos between substantive competition, consumer, and data protection rules and enforcement should not be dismantled altogether. What *is* necessary is ensuring the interoperability of these rules and creating an appropriate institutional structure, operationalizing coordination between three types of authorities at the domestic and EU levels. Focusing on the latter, in this article, we propose a prototype for this institutional structure.

This article is organized as follows. Section 2 details the interplay between the goals and substantive rules of competition, consumer and data protection law in the digital age, and demonstrates how it results in kaleidoscopic enforcement. Section 3 maps out the drawbacks of kaleidoscopic enforcement. Section 4 proposes an institutional solution to address those drawbacks and explains why current efforts to tackle the issue are insufficient. Section 5 concludes.

2. Kaleidoscopic enforcement of competition, consumer and data protection law

Data is crucial for a company to achieve commercial success, as it is routinely used to offer products and services to customers. This makes data collection and use subject to competition and consumer law. At the same time, personal data is also the subject matter of a binding fundamental right to the protection of personal data, as outlined in the EU Charter of Fundamental rights.[25] In the quest for data, every stakeholder – companies and citizens alike – is confronted with data protection law as codified in the EU General Data Protection Regulation (GDPR).[26] Because of the all-embracing interpretation

24. Kerber makes this argument about the protection of privacy interests, but we believe this is true also for protection of competition and consumers. See Kerber, "Digital markets, data, and privacy: Competition law, consumer law and data protection", 11 *Journal of Intellectual Property Law & Practice* (2016), 857.

25. Art. 8 of the EU Charter of Fundamental Rights (EU Charter); Lynskey, "From market-making tool to fundamental right: The role of the Court of Justice in data protection's identity crisis" in Gutwirth et al. (Eds.), *European Data Protection: Coming of Age* (Springer, 2013), pp. 59–84.

26. O.J. 2016, L 119/1–88.

of personal data[27] by data protection authorities (DPAs) and the ECJ,[28] the borderline between personal and non-personal data is increasingly blurred.[29] In the digital environment, where almost any data can be linked to an identifier, the distinction between what constitutes personal data and what remains non-personal data – and therefore not subject to the scrutiny of stringent data protection rules – is often difficult to make.[30] The GDPR has thus become the "law of everything" in the sense that it applies to almost any collection and any use of data.[31] As a result, in any data-related enforcement action by competition or consumer authorities – or any other authority for that matter – data protection rules apply.

The root causes of kaleidoscopic enforcement, as we see them, are the overlapping yet divergent normative rationales and goals of competition, consumer, and data protection law. These increasingly result in the possibility of simultaneous application of two or more of these areas of law to the same behaviour, and insufficient coordination between public authorities of each three areas of law in enforcement cases following such simultaneous application. As the next section shows, a hard conflict between substantive rules is one, but not the only, example of situations where kaleidoscopic enforcement occurs.

27. Art. 4(1) GDPR: "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.

28. Case C-131/12, *Google Spain and Google*, EU:C:2014:317, para 34; Case C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, EU:C:2018:388, para 28; Case C-40/17, *Fashion ID GmbH & Co*, EU:C:2019:629, para 66.

29. Purtova, "The law of everything. Broad concept of personal data and future of EU data protection law", (2018) *Law, Innovation and Technology*, 40–81, at 41, 45–59, arguing that "literally any data can be plausibly argued to be personal", even data about weather.

30. Recital 9 of Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 Nov. 2018 on a framework for the free flow of non-personal data in the European Union, O.J. 2018, L 303. Constantly improved re-identification techniques further complicate the issue by limiting the opportunities of rendering data non-personal through anonymization, which would allow it to escape the scrutiny of stringent data protection laws. For discussion of this, see Tene and Polonetsky, "Big data for all: Privacy and user control in the age of analytics", 11 *Northwestern Journal of Technology and Intellectual Property* (2013), 239; Kondor et al., "Towards matching user mobility traces in large-scale datasets", (2018) *IEEE Transactions on Big Data*; Schwartz and Solove, "The PII problem: Privacy and a new concept of personally identifiable information", 84 *New York University Law Review* (2011), 1814; Purtova, op. cit. *supra* note 29, 78; Ohm, "Broken promises of privacy: Responding to the surprising failure of anonymization", 57 *UCLA Law Review* (2010), 1701, 1706, warning about the problems of re-identification of personal data and stressing that even truly anonymized personal data at some point in time may be re-identified.

31. Purtova, op. cit. *supra* note 29.

2.1. *The root causes of kaleidoscopic enforcement*

Each of these three areas (competition law,[32] consumer law,[33] and data protection[34]) has its own specific goals. Besides their specific goals, all three areas of law serve the common goal of an internal market in the EU.[35] While competition and consumer law constitute, by nature, economic regulation aimed at enhancing social welfare,[36] data protection has its origins in fundamental rights. Although data protection also contributes to promoting social welfare, the fundamental rights rationale of the EU framework requires

32. As well as increasing consumer welfare, EU competition law also tries to contribute to the integration of the internal market. See *infra* note 35. Furthermore, recently fairness is gaining a prominent position in competition law enforcement. See the speech of Vestager on Fairness and competition of 25 Jan. 2018 given at the GCLC Annual Conference in Brussels, <wayback.archive-it.org/12090/20191129212136/https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/fairness-and-competition_en>. Director General of the DG Competition Laitenberger indicated that "fairness has always been a value underpinning EU competition law and its enforcement" since it prohibited unfair prices and trading conditions as of the beginning. Speech of 20 June 2018 at the British Chambers of Commerce EU & Belgium <ec.europa.eu/competition/speeches/text/sp2018_10_en.pdf>; see further Gerard, Komninos and Waelbroeck (Eds.), *Fairness in EU Competition Policy: Significance and Implications* (Larcier, 2020).

33. The goals of EU consumer law are twofold: they intend to ensure that "all consumers in the Community enjoy a high and equivalent level of protection of their interests and to create a genuine internal market"; Recital 9 of Directive 2008/48 on consumer credits, O.J. 2008, L 133/66, and similarly Recital 2 of Directive 1993/13 on unfair terms in consumer contracts, O.J. 1993, L 95/29 and confirmed by Case C-290/19, *RN* v. *Home Credit Slovakia*, EU:C:2019:1130, para 28, and Case C-478/99, *Commission* v. *Sweden*, EU:C:2002:281, para 12.

34. For an overview of the goals of data protection, see Bygrave, *Data Privacy Law: An International Perspective* (OUP, 2014), pp. 117–126.

35. The ECJ has repeatedly held that the goal of EU competition law is not only the protection of competition and consumer welfare but also to "achieve the integration of national markets through the establishment of a single market". See Case C-468/06, *Sot. Lélos kai Sia* v. *GlaxoSmithKline*, EU:C:2008:504, paras. 65–66; Joined Cases C-501, 513, 515 & 519/06 P, *GlaxoSmithKline Services Unlimited* v. *Commission*, EU:C:2009:610, para 61. Regarding market integration role of consumer law, see Stuyck, "European consumer law after the Treaty of Amsterdam: Consumer policy in or beyond the internal market?", 37 CML Rev. (2000), 367–400. On the data protection side, despite a close focus on fundamental rights protection, internal market integration, although no longer the formal legal ground for EU competence to regulate data protection, is still an important component of the European data protection framework. See Art. 16(2) TFEU, Art. 1(1) GDPR and Recital 2 of the GDPR. Furthermore, the GDPR is one of the pillars of the Digital Single Market project, presented by the Commission as the key for making the EU thrive in the emerging global data economy. See Commission Communication, "Completing a trusted digital single market for all", COM(2018)320, at p. 4. See also Costa-Cabral and Lynskey, op. cit. *supra* note 15, 6.

36. This is one of the main goals shared by most competition regimes. Cf. Albæk, "Consumer welfare in EU competition policy" in Heide-Jørgensen et al. (Eds.), *Aims and Values in Competition Law* (DJØF Publishing, 2013), p. 67. However, it is not the only goal.

a higher level of data protection than would be required from a strictly economic perspective.[37] In this article we focus on the relationship between them. The interplay between competition and consumer law can be compared to a rocket about to launch in two stages. In the first stage, competition law creates a choice for consumers on price and quality with the aim to secure lower prices[38] and/or higher quality[39] of products and services. In the second stage, consumer law aims to protect consumers (generally considered the weaker party *vis-à-vis* a business) by guaranteeing them a choice in terms of price[40] and protecting them by imposing quality and safety standards.[41]

It is therefore often assumed that competition law and consumer law mutually reinforce each other.[42] Data protection, in turn, adds an additional layer of protection, safeguarding individual *control* over personal data and choices in terms of how much personal data to share with goods and service providers. This individual rights protection is not instrumental to achieving other goals, such as enhancing social welfare. Rather, it is inextricably linked

37. For an elaborate discussion, see Yakovleva, "Privacy protection(ism): The latest wave of trade constraints on regulatory autonomy", 74 *University of Miami Law Review* (2020), 416, 507–515.

38. A lower price can be achieved by e.g. producing more efficiently and by process innovation.

39. A higher quality can be reached by product/service innovation.

40. E.g. by having requirements on price transparency or (misleading) information. These require traders to mention the correct or complete prices, e.g. in cases on tyres (ACM, "ACM dwingt juiste prijsvermelding autobanden af", 14 Feb. 2019, <www.acm.nl/nl/publicaties/acm-dwingt-juiste-prijsvermelding-autobanden-af>), second-hand cars (ACM, "Advertentieprijzen tweedehands auto's duidelijker na optreden ACM", 21 Aug. 2019 <www.acm.nl/nl/publicaties/advertentieprijzen-tweedehands-autos-duidelijker-na-optreden-acm>), car and building equipment rental by Bo-rent ("Bo-Rent vermeldt prijzen voortaan duidelijker", 11 Aug. 2018, <www.acm.nl/nl/publicaties/advertentieprijzen-tweedehands-autos-duidelijker-na-optreden-acm>), Seats&Sofa's (ACM, "ACM beboet meubelverkoper Seats and Sofas voor misleidende prijzen", 7 June 2018, <www.acm.nl/nl/publicaties/acm-beboet-meubelverkoper-seats-and-sofas-voor-misleidende-prijzen>) and Belvilla holiday home rental (ACM, "Boete voor Belvilla voor misleidende prijsvermelding", 17 Jan. 2018, <www.acm.nl/nl/publicaties/boete-voor-belvilla-voor-misleidende-prijsvermelding>).

41. E.g. where a tour operator did not offer a guarantee (ACM, "ACM beboet reisaanbieder zonder garantiemaatregelen", 10 Jan. 2019, <www.acm.nl/nl/publicaties/acm-beboet-reis aanbieder-zonder-garantiemaatregelen>) and Volkswagen for not living up to the promised environment-friendly diesel cars in Diesel-gate (ACM, "ACM beboet Volkwagen voor misleiding bij dieselaffaire", 28 Nov. 2017, <www.acm.nl/nl/publicaties/acm-beboet-volkswagen-voor-misleiding-bij-dieselaffaire>).

42. Albors-Llorens, "Competition and consumer law in the European Union: Evolution and convergence", 33 YEL (2014), 163. This assumption is however challenged by Cseres in *Competition Law and Consumer Protection* (Kluwer Law International, 2005), p. 49.

to the protection of human dignity.[43] While competition and consumer laws regulate the use of data – only to the extent that it affects competition and/or consumers – data protection regulates the collection and use of personal data in general. Although personal data cannot be reduced to a mere commodity or consideration for a service,[44] in certain cases the amount of personal data collected from individuals by a service provider (as in two-sided markets, such as social media services) can be compared to a price.[45] From this perspective, competition, consumer, and data protection laws have the overlapping goals of empowering individuals to make choices on price and quality (where personal data can be both a substitute for price and a characteristic of quality) and addressing power asymmetries.[46] On the other hand, competition and data protection laws contrast with one another in terms of their approach to data flow: while the primary aim of data protection law is to limit its disclosure, from the perspective of competition law, such disclosure is viewed as beneficial for competition since all undertakings can then offer and improve existing products or services and/or innovate new products or services with the data.[47]

Three different types of enforcement agencies enforce competition, consumer, and data protection laws, reflecting the three policy areas concerned with the use of personal data. Competition authorities have a role to play because of the impact that personal data has on competition between undertakings. Consumer authorities also carry out enforcement against the unfair use of consumers' personal data. In a few of the EU Member States, such as Austria and Germany, enforcement of consumer law is mostly left to

43. Explanations Relating to the Charter of Fundamental Rights, O.J. 2007, C 303/02, explanation 1.

44. EDPS Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, p. 3.

45. See e.g. Bataineha et al., op. cit. *supra* note 13, 472.

46. See e.g. Esayas, "Data privacy in European merger control: Critical analysis of Commission Decisions regarding privacy as a non-price competition", 4 ECLR (2019), 166.

47. On the pro-competitive aspect of data-sharing see Crémer, De Montjoye and Schweitzer, op. cit. *supra* note 15, p. 8; and on the protection of data in case of data sharing, see the view of the EDPS: Wiewiórowski, "Sharing is caring? That depends …", 13 Dec. 2019 <edps.europa.eu/press-publications/press-news/blog/sharing-caring-depends_en>. The UK Competition & Markets Authority is even worried that the GDPR can create an artificial barrier to competition; the CMA worries "that Google and Facebook have a clear incentive to apply a stricter interpretation of the requirements of data protection regulation when it comes to sharing data with third parties than for the use and sharing of data within their own ecosystems". Therefore the CMA wants to cooperate closely with the UK DPA, Information Commissioner's Office (ICO), "to consider the appropriate approach", CMA, "Online platforms and digital advertising, Market study final report", 1 July 2020, para 5.329–330. See also e.g. Graef, "Limits and enablers of data sharing: An analytical framework for EU competition, data protection and consumer law", TILEC Discussion Paper, DP 2019-024, 11–12, 17–18.

private enforcement by consumer organizations and individuals; in several others, such as the Netherlands and France, consumer organizations play a major role in consumer law enforcement on a par with public authorities.[48] Finally, DPAs are vested with supervisory and enforcement powers under the GDPR.[49] Since the GDPR took effect, private enforcement of the GDPR by individuals and NGOs, including consumer organizations, is on the rise.[50] Supervisory authorities in the three policy areas have recently begun to factor in the peculiarities of the data economy when initiating and carrying out enforcement actions. However, enforcement actions against unlawful data processing practices under competition or consumer law do not have the direct purpose of protecting individuals' rights to personal data. Instead, they aim to protect competition and consumer interests. At the same time, although competition and consumer authorities or courts – in cases of private enforcement of consumer law – do not *directly* enforce the GDPR, the business practices they curtail could often – independently of these competition or consumer violations – simultaneously qualify as violations of the data protection law.

As mentioned in the introduction, there are primarily at least two types of interactions in the enforcement of competition, consumer, and data protection rules in data-related contexts: parallel enforcement actions and internalizing the rules of one area of law to further the goals of the other. The following two sections provide examples of each of these modes of interaction.

2.2. *Parallel enforcement actions*

In light of the overlapping goals of ensuring consumer choice on how personal data is collected and used, and tackling power asymmetry between consumers

48. Faure and Weber, "The diversity of the EU approach to law enforcement – Towards a coherent model inspired by a law and economics approach", 18 GLJ (2017), 831; Nessel, "Consumer policy in 28 EU Member States: An empirical assessment in four dimensions", 42 *Journal of Consumer Policy* (2019), 457.

49. Art. 51 GDPR.

50. E.g. mass claims for data privacy violations against Facebook are pending in several EU Member States. See e.g. Dutch News, "30,000 Facebook users join mass compensation claim for breach of privacy", 7 July 2020, <www.dutchnews.nl/news/2020/07/30000-facebook-users-join-mass-compensation-claim-for-breach-of-privacy/>; Gladicheva, "Facebook's snarling of European data-breach lawsuits shows limits of private enforcement", MLEX Market Insight, 9 March 2020, <mlexmarketinsight.com/insights-center/editors-picks/area-of-expertise/data-privacy-and-security/facebooks-snarling-of-european-data-breach-lawsuits-shows-limits-of-private-enforcement>; De Brauw Blackstone Westbroek, "Class action exposure: A growing threat to companies dealing with consumer data", 28 Jan. 2020, <www.debrauw.com/download/25517/>.The question whether consumer organizations that have not been mandated by individuals have standing in claims under the GDPR was referred to the ECJ by the German Federal Court of Justice on 28 May 2020, Decision No. I ZR 186/17. Case C-319/20, *Facebook Ireland*.

and businesses, consumer and data protection laws rely on transparency rules to achieve their objectives.[51] Transparency is one of the overarching principles of EU data protection law, laid down in Articles 13 and 14 of the GDPR. These provisions provide lists of information that data controllers must communicate to individuals before processing their personal data. The GDPR also requires that such information be concise, transparent, intelligible and easily accessible, and provided in clear and plain language.[52] Independent of the GDPR rules, EU consumer law also has requirements (in the context of providing goods or services where personal data is a component or where it is related to personal data collection in other ways) on informing individuals about how their data is collected and used. The European Data Protection Supervisor (EDPS) and several scholars argue that providing insufficiently clear or unintelligible information about how consumers' personal data is collected and used could constitute unfair commercial practice, thus violating consumer rights under the Consumer Rights Directive, or misleading advertisement.[53]

These two sets of rules apply in parallel to the same data collection practices – and therefore could be enforced independently of each other – by consumer and data protection authorities in one or several EU Member States.[54] For example, in two separate cases against Facebook, Italian and Hungarian consumer protection authorities each decided that Facebook's claim that its services are free, while at the same time, using individuals' data for commercial purposes, constitutes unfair commercial practice, and imposed fines of EUR 10 million and EUR 3.6 million respectively.[55] In its decision (recently confirmed by the Administrative Tribunal of Lazio following

51. Helberger, Zuiderveen Borgesius and Reyna, op. cit. *supra* note 15, 1438–1439.

52. Art. 12 GDPR; Art. 29 Working Party, Guidelines on transparency under Regulation 2016/679 (WP 260), 22 Aug. 2018, p. 6.

53. See in more detail EDPS Opinion 8/2016, cited supra note 15, pp. 24–25; Kerber, op. cit. supra note 24, 857 and 862; Helberger et al., op. cit. supra note 15, 1428–1429 and 1438–1440; Guidelines cited supra note 52, p. 4.

54. Helberger et al., op. cit. *supra* note 15, at 1428–1429; Kerber, op. cit. *supra* note 24, 857; Guidelines cited, *supra* note 52, p. 4.

55. *Autorità Garante della Concorrenza e del Mercato* (Italian Competition and Consumer Authority) "Facebook fined 10 million Euros by the ICA for unfair commercial practices for using its subscribers' data for commercial purposes", 7 Dec. 2018, <en.agcm.it/en/media/press-releases/2018/12/Facebook-fined-10-million-euros-by-the-ICA-for-unfair-commercial-practices-for-using-its-subscribers%E2%80%99-data-for-commercial-purposes>; "Italy threatens to fine Facebook in data disclosure row", *Financial Times* 24 Jan. 2020, <www.ft.com/content/bd17beec-3e7d-11ea-b232-000f4477fbca>; Hungarian Competition Authority, "GVH imposed a fine of EUR 3.6M on Facebook", 6 Dec. 2019, <www.gvh.hu/en/press_room/press_releases/press_releases_2019/gvh-imposed-a-fine-of-eur-3.6-m-on-facebook>.

Facebook's appeal),[56] the Italian consumer authority explicitly stated that the fact that Facebook's conduct also falls under the personal data protection law does not exempt it from complying with rules on unfair commercial practices. The Italian authority noted that these two areas of law are not in conflict, but instead, complement each other. While a DPA can engage in enforcement with a view to the protection of fundamental rights, the consumer authority does so in order to protect consumers' economic choices from deceptive and aggressive practices.[57] In relation to an investigation by the Irish DPA against Facebook in 2011–2012, the Italian authority noted that such investigation was conducted under a regulatory framework that differed from the *ex post* unfair commercial practices rules in the Italian Consumer Code.[58] The possibility of simultaneously applying consumer and data protection rules to the same behaviour has also been recently demonstrated by the Chamber Court of Berlin which found Facebook's terms and conditions, among other things, to be inconsistent with both consumer and data protection laws.[59]

Another category of parallel enforcement cases derives from the divergent goals of competition and data protection law in terms of personal data flows. European and national competition authorities, as well as the European Commission, have repeatedly stated that requiring data monopolists to share data with competitors could be a viable measure to enhance competition in the digital market and to increase availability of data for training AI systems.[60] These practices, however, conflict with the GDPR's goal to maximize individuals' control over their data. Several examples illustrate the point.

Recently, various DPAs throughout Europe have issued guidance condemning – as potentially unlawful from the GDPR perspective – the existing practices of collecting personal data through third-party cookies and

56. IAPP, "The economic exploitation of personal data in privacy and consumer laws", 24 March 2020, <iapp.org/news/a/the-economic-exploitation-of-personal-data-in-privacy-and-consumer-laws/>.

57. Decision of 29 Nov. 2018 of *Autorità Garante della Concorrenza e del Mercato,* in relation to Facebook Inc. and Facebook Ireland Ltd., see press release *supra* note 55, paras. 45–46.

58. Ibid., para 48.

59. Judgment of Berlin Chamber Court of 27 Dec. 2019, 16O341/15, <www.vzbv.de/sites/default/files/downloads/2020/01/24/kg_20.12.2019.pdf>.

60. COM(2020)66 final, *supra* note 6, at p. 14; Euractiv, "Vestager calls for more access to data for smaller platforms", 10 May 2019, <www.euractiv.com/section/data-protection/news/vestager-calls-for-more-access-to-data-for-small-platforms/>; Costa-Cabral and Lynskey, op. cit. *supra* note 15, at 3–4; Graef, Clifford and Valcke, op. cit. *supra* note 15, at 213. See also a policy letter of the State Secretary of Economic Affairs and Climate of 17 June 2019 to the Dutch Parliament (Upper Chamber) about future-proof competition enforcement instruments with regard to online platforms. In the annex, the State Secretary mentions that the general obligation to share data not only constitutes a violation of the GDPR, but also creates incentives for platforms to curb innovation and investment, *Eerste Kamer* 2018–2019, 34 978, D, p. 25.

similar software, and onward-sharing that data with numerous ad tech providers.[61] Following this guidance, several DPAs have started investigations into, followed by enforcement actions against, the use of third-party cookies by websites.[62] At the same time, in a move to build "a more private web", Google and Apple announced that they will block all third-party cookies on their Chrome and Safari web browsers.[63] While this is a privacy enhancing measure – when seen from a data protection perspective – Google's announcement quickly raised competition law concerns and suspicions that by not allowing third-party cookies, the tech giant is merely trying to favour its own services over its competitors.[64] A similar dilemma arises when a remedy enhancing competition conflicts with data protection law – the most obvious example being data sharing. In a recent judgment, a Dutch court forced the Dutch Authority for Consumers and Markets to bring its Electricity and Gas Information Code into compliance with the GDPR.[65] The mandatory and unconditional manner in which the Code required network operators to share personal data with suppliers, obtained from smart meters, did not have a valid legal basis under the GDPR.[66] In the regulatory landscape, this conflict has been resolved in a similar manner. Under the Payment Services Directive (PSD2), which seeks to stimulate competition and innovation in the payment services market, banks are required to share individuals' account information, which qualifies as personal data. However, banks may only do so if they are in full compliance with the GDPR; in other words, if it is strictly necessary for

61. See e.g. ICO Guidance on the use of cookies and similar technologies, 3 July 2019, <ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf>; CNIL Guidelines on cookies and tracking devices, 4 July 2019, <www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038783337> (in French).

62. See e.g. the investigation by the Dutch DPA, <autoriteitpersoonsgegevens.nl/nl/nieuws/ap-veel-websites-vragen-op-onjuiste-wijze-toestemming-voor-plaatsen-tracking-cookies>.

63. Schuh, "Building a more private web", Chrome, 22 Aug. 2019, <www.blog.google/products/chrome/building-a-more-private-web/>; Statt, "Apple updates Safari's anti-tracking tech with full third-party cookie blocking", *The Verge,* 24 March 2020, <www.theverge.com/2020/3/24/21192830/apple-safari-intelligent-tracking-privacy-full-third-party-cookie-blocking>.

64. Scott, "Google's renewed privacy push raises tough antitrust questions", *Politico*, 16 Jan. 2020, <www.politico.eu/article/google-privacy-competition-chrome-publishers-online-advertising-antitrust/>. In contrast, Robertson argues that from a competition law perspective, excessive data collection via third-party tracking could constitute an unfair trading conditions abuse, and therefore violate EU competition law. See Robertson, op. cit. *supra* note 15, 178–183.

65. The Dutch Trade and Industry Appeals Tribunal (CBB) judgment of 14 Jan. 2020, NL:CBB:2020:3 (in Dutch).

66. Ibid., paras. 4.2–4.3. (The court held that "In order to implement the cited provisions of the Information Code, network operators must have a (different) valid processing basis in the GDPR. That the ACM has formulated these provisions compulsorily (and unconditionally) is not compatible with this" (our translation).

the performance of the contract between the individual to whom this data relates, and the payment service provider.[67]

Conversely, the GDPR and EU data protection authorities welcome drawing up an industry-wide data protection code of conduct. Adherence to such a code of conduct is viewed by the GDPR as one of the ways to best demonstrate data protection compliance.[68] Aligning the data protection policies of industry participants may result in questionable practices from a competition law perspective, in that it could hamper the ability of certain market players to adhere to the code of conduct (for example, by setting too high a standard) or it could lead to market players being viewed as cartels.[69]

2.3. *Internalizing the rules of one area of law to further the goals of another area of law*

In addition to parallel enforcement, competition, consumer and data protection law also interact when enforcement authorities internalize the concepts of one area of law to interpret and further the goals of the other. The most prominent example of internalizing data protection rules by a competition authority is the 2019 case of the German competition authority against Facebook. In its decision – currently under appeal – the German competition authority found that the collection and combination of personal data by Facebook without the explicit and voluntary consent of its users was

67. The question remains whether consent within the meaning of PSD2 is the same form of consent as the explicit consent required under the GDPR. The EDPB is of the opinion that consent within the meaning of Art. 94(2) PSD2 is "merely" consent in the contractual relationship between the payment service provider and its customer and is therefore deemed to be consent for the performance of that contract within the meaning of Art.(1)(b) GDPR and not a separate explicit consent within the meaning of Art. 6(1)(a) GDPR. See EDPB, Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR (version for public consultation), 16 Sept. 2020, 8.

68. Recital 81, Art. 28(5) and Art. 32(3) GDPR. E.g. the UK ICO "is committed to encouraging the development of codes of conduct". The regulator sees "a real benefit to developing a code of conduct as it can help to build public trust and confidence in your sector's ability to comply with data protection laws". ICO, "Codes of Conduct", <ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/>.

69. See e.g. Federle and Eckhardt Descout, "The interplay of data protection and competition law – issues beyond the Facebook case", Bird&Bird, March 2019, <www.twobirds.com/en/news/articles/2019/global/the-interplay-of-data-protection-and-competition-law-issues-beyond-the-facebook-case>; De Brauw Blackstone Westbroek, "Our IAPP panel on convergence of data-related enforcement in digital age – key insights", 16 Dec. 2019, <www.debrauw.com/legalarticles/our-iapp-panel-on-convergence-of-data-related-enforcement-in-digital-age-key-insights/>.

abusive from a competition law perspective.[70] And since Facebook has a dominant position, this behaviour violated the prohibition against abuse of a dominant position. Although this decision is based on German case law, where the violation of fundamental rights by dominant companies also constitutes illegal abuse of a dominant position under competition law,[71] the same outcome could be reached based on Article 102 TFEU.[72] This case ties into the broader trend, in Europe and beyond, of resorting to competition law to address data privacy and governance issues; it has a potential to mark a watershed in the relationship between data protection and competition law in the future. Given its importance, it is possible that the question of whether and to what extent a violation of data protection can be used to define a violation of competition law may ultimately be referred to the ECJ.

In addition, several scholars argue that data protection concepts could provide a benchmark for assessing fairness of consumer contracts – which require individuals to share data with goods or services providers under the Unfair Contract Terms Directive – by consumer authorities.[73] In this case, a contract could be considered unfair, for example, if it: breaches the GDPR's data minimization principle or users' security or privacy in its default requirements; abuses consent as a legitimate ground for personal data

70. Decision B6-22/16 of 6 Feb. 2019. On appeal, the *Oberlandesgericht Düsseldorf* was at first sight not sure whether this analysis is correct and suspended the obligations the German Federal Cartel Office imposed on Facebook (Judgment VI-Kart 1/19 (V) of 26 Aug. 2019, *Bundeskartellamt*). This suspension was overturned by the German Supreme Court (Decision of 23 June 2020, KVR 69/19), which concluded that there are no serious doubts about Facebook's dominant position in the German social network market or that Facebook is abusing this dominant position with the terms of use prohibited by the Cartel Office. As the next step, *Oberlandesgericht Düsseldorf* will decide on the substance of the case. Colangelo and Maggiolino criticize a direct reference to data protection law in the assessment of exploitative abuse because this creates "an automatism consisting of the idea that a digital platform abuses its dominant market power whenever it violates privacy law". This, in their opinion, will ultimately lead to personal data protection becoming one of the objectives of competition law, and will allow competition authorities to find that joint violations of data protection decided by several companies is an anticompetitive agreement, or that a merger substantially lessens competition if it leads to a creation of market power allowing to impose contractual terms violating privacy. Colangelo and Maggiolino, "Manipulation of information as antitrust infringement", (2019) CJEL, 367 (forthcoming), available at <ssrn.com/abstract=3262991>.

71. *Bundesgerichtshof* judgment of 6 Nov. 2013, VBL-Gegenwert (KZR 58/11) and *Bundesgerichtshof* judgment of 7 June 2016, *Pechstein/International Skating Union* (KZR 6/15); Robertson, op. cit. *supra* note 15, 185.

72. Volmar and Helmdach, "Protecting consumers and their data through competition law? Rethinking abuse of dominance in light of the federal cartel office's Facebook investigation", 14 *European Competition Journal* (2018), 195–215, 202.

73. Helberger et al., op. cit. *supra* note 15, 1449–1451; Rott, "Data protection law as consumer law – How consumer organisations can contribute to the enforcement of data protection law", 6 *Journal of European Consumer and Market Law* (2017), 114.

processing; or if privacy policies are not phrased in plain and intelligible language.[74] Conversely, the consumer law fairness test can be used to interpret the principles of data minimization and purpose limitation as outlined in data protection law.[75]

In a similar vein, data protection law could serve as a normative benchmark or give context in interpreting competition law's concept of fairness under Article 102 TFEU, non-price parameters of competition under Articles 101 and 102 TFEU, or in merger control.[76] It could also provide a "normative yardstick for assessing competition on data processing in all its dimensions – not only quality, but also choice and innovation".[77] In their analysis, Costa-Cabral and Lynskey stress that internalizing data protection rules as methods of interpreting competition law concepts would not require expanding the notion of consumer welfare, but would merely provide an "insight into the normative backdrop for competitive activity".[78] In other words, competition law will use data protection as an instrument to achieve its own goals, as opposed to those of data protection law.[79] In data protection, the competition law concept of dominance could be used to scale up a dominant company's data protection obligations through the GDPR's accountability principle,[80] which was itself borrowed from competition law.[81] In fact, several scholars contend that dominant firms should be subject to a more stringent data protection standard for the collection of personal data.[82] In this case, DPAs would internalize competition law's concept of dominance.

74. Ibid.

75. Helberger et al., op. cit. *supra* note 15, 1451.

76. Costa-Cabral and Lynskey, op. cit. *supra* note 15, 3–4, 20; Graef, Clifford and Valcke, op. cit. *supra* note 15, 213; Kalimo and Majcher, "The concept of fairness: Linking EU competition and data protection law in the digital marketplace", 42 EL Rev. (2017), 219; Robertson, op. cit. *supra* note 15, 178–183; Walters, Zelles and Trakman, "Personal data law and competition law – where is it heading?", (2018) ECLR, 505. Volmar and Helmdach, op. cit. *supra* note 72, 214; Gerard, Komninos and Waelbroeck, op cit. *supra* note 32.

77. Costa-Cabral and Lynskey, op. cit. *supra* note 15, 16; see also Carugati, op. cit. *supra* note 19, 7, arguing that incorporating data protection concerns in the assessment of exploitative abuse of dominance is possible through a new theory of harm based on the relationship between market dominance and data protection.

78. Costa-Cabral and Lynskey, op. cit. *supra* note 15, 3–4.

79. Ibid., 17. In contrast, Kalimo and Majcher argue that reference to data protection law in assessing exploitative abuse would require broadening the scope of Art. 102 and making the concept of "abuse" more "open-ended" or "nebulous". See Kalimo and Majcher, op. cit. *supra* note 76, 228.

80. Art. 5(2) GDPR.

81. EDPS Opinion 8/2016, cited *supra* note 15, p. 7.

82. Kuner et al., "When two worlds collide: The interface between competition law and data protection", 4 *International Data Privacy Law* (2014), 247; Crémer, De Montjoye and Schweitzer, op. cit. s*upra* note 15, p. 80.

3. Kaleidoscopic enforcement drawbacks

Kaleidoscopic enforcement, we argue, has the following three key drawbacks: (i) undermining coordination mechanisms within each individual area of law; (ii) incoherent enforcement of EU law; and (iii) under-enforcement or over-enforcement of data-related practices. We discuss each of these drawbacks in the following sections.

For a more nuanced picture, we first address the possible positive aspects of kaleidoscopic enforcement. Some scholars argue that in certain cases, enforcement by competition or consumer authorities is welcome, and could make up for the weaknesses of the data protection regime, which, in Purtova's words, is "highly intensive and non-scalable".[83] By way of example, consumer law transparency rules are more flexible and adaptable than their rigid data protection counterparts. Therefore, they can more effectively address information asymmetries between companies and consumers.[84] This, in turn, strengthens individuals' rights and interests.[85] Beyond the information requirements, Helberger, Zuiderveen Borgesius and Reyna also note that the fairness of consumer law under the Unfair Contract Terms Directive[86] could compensate for the limited ability of data protection law to protect individuals from abuse of consent as a legitimate ground for data processing under the GDPR.[87] Even when the GDPR's consent rules are met, the collection of personal data could still be found to violate consumer law. Similarly, several authors view competition law as a "silver bullet which will render data protection rules more effective".[88]

While below we focus on the drawbacks of kaleidoscopic enforcement, we do not argue against it. Instead, by explicitly addressing its drawbacks, we create a stepping-stone towards finding a solution – an institutional mechanism – which would minimize the social costs of kaleidoscopic enforcement, without diminishing its benefits.

83. Purtova, op. cit. *supra* note 29, 75–78.

84. Van Eijk, Hoofnagle and Kannekens, "Unfair commercial practices: A complementary approach to privacy protection", 3 *European Data Protection Law Review* (2017), 325–337, 11–12; Helberger et al., op. cit. *supra* note 15, 1438–1439.

85. Helberger et al., op. cit. *supra* note 15, 1428–1429, 1438–1440; Kerber, op. cit. *supra* note 24, 861, 862–864; Costa-Cabral and Lynskey, op. cit. *supra* note 15, 11–50.

86. Directive 93/13/EEC on unfair terms in consumer contracts (Unfair Contract Terms Directive), O.J. 1993, L 95/29.

87. Helberger et al., op. cit. *supra* note 15, 1451.

88. Kuner et al., op. cit. *supra* note 82, 247. See also Crémer, De Montjoye and Schweitzer, op. cit. *supra* note 15, p. 52.

3.1. *Undermining coordination mechanisms within each individual area*

The carrying out of enforcement actions by two or more authorities in *different* EU Member States for the same data processing practice could bypass the coordination of existing mechanisms in each of the three areas of law.

Despite more interaction between substantive competition, consumer, and data protection rules, supervisory and enforcement authorities largely operate in silos. This "silo effect" has a great deal to do with their limited mandate to enforce a specific area of law, their organizational structures, rules of procedure and their limited financial resources. Formal cooperation mechanisms between authorities are also limited to specific areas. Consistency of application and enforcement of data protection law throughout the EU is ensured by the one-stop-shop and the cooperation and consistency mechanisms under the GDPR.[89] The one-stop-shop mechanism allows multinational companies to deal with only one "lead" DPA, which is determined based on the location of the company's main establishment in the EU.[90] Other EU DPAs can only enforce data protection rules against these companies in a limited set of cases.[91] The cooperation mechanisms require DPAs to cooperate in enforcement actions, exchange information, share and comment on draft decisions, and provide mutual assistance in GDPR enforcement.[92] The consistency mechanism allows for the resolution of disputes between DPAs on the interpretation and application of the GDPR.[93]

To achieve the effective and consistent application of EU competition law, European competition law has created a one-stop-shop system within merger control, and a cooperation system between the European Commission and national competition authorities in the European Competition Network (ECN) for antitrust cases, which includes the prohibition of cartels under Article 101

89. Arts. 60–67 GDPR.

90. Art. 56 GDPR, Art. 29 Data Protection Working Party, Guidelines for identifying a controller or processor's lead supervisory authority, 13 Dec. 2016, WP 244 rev. 01.

91. These cases are: (i) if a DPA contests the company's claim that their main establishment is in another EU Member State; e.g. this has been done by CNIL in the investigation against Google, see CNIL, cited *supra* note 7; (ii) when there is no cross-border data processing (which is almost never the case; under Art. 56 GDPR, the one-stop-shop mechanism only applies to cross-border processing of personal data); (iii) when there is an urgent need to protect the rights and freedoms of affected individuals, a DPA can use its powers under Art. 66 GDPR to adopt provisional measures with a maximum period of validity of 3 months. The Hamburg Data Protection Commission is currently using this power to prohibit Google from carrying out evaluations of their voice assistant programme by employees and third parties. See Womble Bond Dickinson, "Hamburg Data Protection Commission: Declaring a data emergency", *JDSupra,* 7 Aug. 2019, <www.jdsupra.com/legalnews/hamburg-data-protection-commission-88306/>.

92. Arts. 60–62 GDPR.

93. Arts. 63–65 GDPR.

TFEU and abuse of dominance under Article 102 TFEU.[94] Within the ECN, the European competition authorities inform each other of new cases and decisions, and collaborate in investigations with one another (e.g. they exchange information and evidence, and share and comment on the draft decisions).

Consumer protection authorities form the Consumer Protection Cooperation network (CPC network), which provides for coordinated investigation and enforcement mechanisms for widespread infringements of consumer law.[95] This mechanism includes a notice system about widespread infringements, exchanging evidence and information during infringement investigations, and the possibility of launching a coordinated action and taking coordinated enforcement measures in all Member States concerned against a widespread infringement.[96]

In the case of kaleidoscopic enforcement by two (or more) different authorities in two (or more) EU Member States, none of these coordination mechanisms applies. The way in which kaleidoscopic enforcement has already affected the one-stop-shop mechanism under the GDPR illustrates how kaleidoscopic enforcement can undermine the coordination mechanisms more generally. Tackling a potential GDPR violation under competition or consumer laws, which are not bound by the GDPR one-stop-shop mechanism, has allowed Member States to initiate enforcement actions when they would otherwise not be able to do so under the GDPR because "their" DPA is not the lead authority. This has been demonstrated by the enforcement actions of Italian and Hungarian consumer authorities and by the German competition authority against Facebook. Because Facebook's lead DPA is in Ireland, DPAs in any of these other EU Member States would not be able to pursue Facebook's practices under the GDPR, as this is the prerogative of the Irish DPA. Framing the issue under consumer or competition law has made

94. The Council and the Commission gave a Joint Statement on the Functioning of the Network of Competition Authorities (15435/02 ADD 1), at the adoption of Regulation 1/2003 (O.J. 2003, L 1/1). A more detailed interpretation of the work of the ECN is given by the Commission in its "Notice on cooperation within the Network of Competition Authorities" (O.J. 2004, C 101/43). There is currently no one-stop-shop mechanism for antitrust cases. It has been suggested that the extension of the one-stop-shop mechanism to the enforcement of antitrust prohibitions would increase consistency in antitrust enforcement, see Hoyng, Chappatte and De Morant, "Achieving consistent outcomes in digital markets: European merger reviews vs. antitrust investigations", *Antitrust Magazine* (Summer 2019), 66.

95. Chapter IV of Regulation (EU) 2017/2394 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) 2006/2004, O.J. 2017, L 345/1.

96. Arts. 17–21 of Regulation (EU) 2017/2394.

enforcement actions in these other EU Member States possible. Although application of data protection rules by other authorities, in principle, does not exclude the involvement of a DPA, this involvement – and the role of the DPA in the enforcement procedure – is left to the discretion of the competition or consumer authority handling the case. It is also not necessarily the case that the lead DPA will be involved. While investigating Facebook under competition law, the German competition authority consulted the German, not the Irish, DPA.[97]

Kaleidoscopic enforcement may also create legal uncertainty as to the amount of a fine for a specific violation. Although the approach to setting fines for data protection violations has been, to some extent, borrowed from EU competition law (e.g. the notion of "undertaking" and the calculation of fines based on an undertaking's turnover),[98] the maximum amount of a fine under competition law is more than double that under data protection law. While a maximum fine for violations of data protection law may be up to 4 percent of global annual turnover, the maximum fine under competition law is up to 10 percent.[99] Or might the result of kaleidoscopic enforcement even be several fines which add up to 14 percent?[100] Companies will face higher fines if competition authorities take enforcement action against a specific personal data processing practice rather than data protection authorities. When it comes to consumer law remedies, most are regulated at the national level which further complicates the matter.[101]

In summary, kaleidoscopic enforcement without proper pan-European cross-disciplinary coordination could hamper EU efforts to achieve consistent interpretation and enforcement of EU law, and further increase transaction costs for companies that will have to navigate different rules and procedures in different EU Member States. The next section elaborates further on this point.

97. *Bundeskartellamt*, Case summary: Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing, B6-22/16, 15 Feb. 2019, <www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4> (explaining the advice the German Competition Authority received from the German data protection authorities and that the Irish DPA was merely "briefed" about the competition authority's proceedings).

98. Rec. 150 GDPR. Art. 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, 3 Oct. 2017, WP253, p. 6.

99. Art. 83 GDPR, Art. 23(2) of Regulation 1/2003. Volmar and Helmdach argue that the difference in fines is one of the reasons why data protection law violations should not be viewed as violations of Art. 102(a) TFEU. Volmar and Helmdach, op. cit. *supra* note 72, 210–211.

100. On the possible limitation of fines under e.g. the *ne bis in idem* principle, see *infra* section 3.3.

101. See e.g. Rott, op. cit. *supra* note 73, 117–119.

3.2. *Incoherent enforcement on the single market*

Besides their specific goals discussed above, competition, consumer and data protection law all serve the common goal of having an internal market in the EU.[102] In addition to the points demonstrated in the previous section, kaleidoscopic enforcement may put this goal at risk in another way: by internalizing the concepts of one area of law to another area of law, different types of authorities, and namesake authorities in different Member States, may use inconsistent interpretation of the same concept.[103] As discussed above, the goals of competition or consumer law overlap only partly with those of data protection. Interpreting data protection concepts through the prism of the goals of their own respective areas of law, competition and consumer authorities may do so differently from the DPAs, thus arriving at a different outcome. To illustrate this point, let us return to the example of the investigation against Facebook by the German competition authority. Facebook was fined under competition law because it had not obtained valid consent from users while collecting their data through social plug-ins on third-party websites. Conversely, in its *Fashion ID* ruling, which was based on EU data protection law, the ECJ decided that it was the website itself, not Facebook, that had to obtain user consent.[104]

Another cause of incoherent enforcement of EU competition, consumer, and data protection rules is their divergent conceptualization of "personal data". On the one hand, from an economic perspective of competition and consumer law, personal data is an economic asset which, in some cases, could be compared to the price of a good or service;[105] on the other hand, from a data protection perspective, it is a subject of fundamental rights and "cannot be

102. See *supra* notes 33–35.

103. See Volmar and Helmdach, op. cit. *supra* note 72, 210–211.

104. Case C-10/17, *FashionID*, EU:C:2019:629, para 102. The ECJ explained that this consent will be limited to the processing of personal data in respect of which the website operator actually determines the purposes and means. Although this means that for some personal data uses Facebook, indeed, may need a separate consent, this is not the case when it comes to the collection and transmission of data from the website operator to Facebook.

105. E.g. Recital 16 of the European Electronic Communications Code clarifies that providing personal or other data to a service supplier or allowing such supplier to access personal data without actively supplying it (an example of this would be online tracking) in exchange for a service falls under the concept of remuneration. See Recital 16, Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 Dec. 2018 establishing the European Electronic Communications Code, O.J. 2018, L 321/36. See also Recital 24 and Art. 3(1) of Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, O.J. 2019, L 136/1.

considered as a mere commodity".[106] As stated elsewhere in this article, Italian and Hungarian consumer authorities held that Facebook's social media service is not "free", as it is "paid" for by users' data.[107] The Italian court, which affirmed the Italian authority's approach, has explicitly noted the inherent tension.[108] Conversely, when considering the same issue from both the consumer and data protection perspective, the Chamber Court of Berlin ruled that such advertising is not misleading – because it merely refers to the absence of cash payments.[109] In other words, the court – unlike the consumer authorities – considered remuneration in a narrow sense.

3.3. *Suboptimal level of enforcement*

In kaleidoscopic enforcement, each authority – except for *ad hoc* coordination – considers the impact of enforcement (or lack of enforcement) by looking only at the specific public policy interests protected by the area of law that it is empowered to enforce. As a result, kaleidoscopic enforcement may lead to under-enforcement or over-enforcement of certain data-related practices.

The most prominent example of under-enforcement is the European Commission's deliberate refusal to take into account the implications for privacy and data protection when tech companies merge – such as *Google/DoubleClick* and *Facebook/WhatsApp* – and their datasets are combined.[110] The European DPAs and the EDPS have voiced the importance of factoring in privacy and data protection into the set of policy interests considered when assessing prospective tech-company mergers.[111] Nevertheless, at the moment of writing, there is still no publicly available example of a successful collaboration between European competition and data protection authorities in a merger case. At the moment of writing, the

106. European Data Protection Supervisor, EDPS Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, p. 3.

107. Ibid.

108. IAPP, op. cit. *supra* note 56.

109. Judgment of Berlin Chamber Court cited *supra* note 59.

110. See Case C-238/05, *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito* v. *Asociación de Usuarios de Servicios Bancarios (Ausbanc)*, EU:C:2006:734. For an overview of the cases, see Costa-Cabral and Lynskey, op. cit. *supra* note 15, 7–8, or Graef, Clifford and Valcke, op. cit. *supra* note 15, 218–219.

111. Statement of the EDPB on privacy implications of mergers, 19 Feb. 2020, <edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_privacyimplicationsofmergers_en.pdf>; Statement of the EDPB on the data protection impacts of economic concentration, <edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_en.pdf>; EDPS Opinion 8/2016, cited *supra* note 15.

Google/Fitbit case is still undergoing merger review by the Commission.[112] This might be, or might have been, a good case to cooperate closely with DPAs because Fitbit holds health data of its users, which is sensitive personal data as the EDPB indicated after the *Apple/Shazam* case.[113] The way in which the Australian competition authority already objected to this take-over makes it painfully clear how deficient data protection under competition law enforcement is, since data protection is not the goal but merely a quality aspect of the service rendered by Fitbit – on which it competes, since it has a "a strong consumer record for data privacy protection, which consumers appear to value".[114] DPAs as well as competition and consumer authorities may still exercise *ex post* enforcement measures against violations of data protection, competition, and consumer law resulting from or following the merger – which, for example, happened in the *Facebook/WhatsApp* case.[115] However, as opposed to *ex ante* merger control, these measures allow to stop a violation but are – most of the time – unable to undo the harm incurred by individuals as consumers and data subjects and the market by the violation.

In contrast, the risk of over-enforcement remains theoretical. It could materialize if different authorities in one EU Member State begin enforcing against the same data-related practice. Over-enforcement may occur if enforcement authorities do not take into account the fines already imposed for the same behaviour by their counterpart(s), leading to a disproportionate total fine.[116] While the doctrine of *ne bis in idem*, also known as double jeopardy, aims to prevent such situations, it is unlikely to apply. This principle only applies if the following three conditions are all met: (i) the same facts; (ii) the same offender; and (iii) the rules, which are violated, protect the same

112. Case M.9660, *Google/Fitbit,* pending. The Commission opened an in-depth investigation because of concerns that Google can increase its market dominance by "increasing the already vast amount of data" by taking over Fitbit <ec.europa.eu/commission/presscorner/detail/en/IP_20_1446>.

113. EDPB statement, cited *supra* note 23.

114. Australian Competition and Consumer Commission, Statement of Issues, 18 June 2020, Google LLC – proposed acquisition of Fitbit Inc., para 143.

115. For an overview, see Carugati, op. cit. *supra* note 19, 4–5. See also "Facebook, WhatsApp fined by Spain for failure to obtain consent", 16 March 2018, *Bloomberg Law*, <news.bloomberglaw.com/business-and-practice/facebook-whatsapp-fined-by-spain-for-failure-to-obtain-consent>; "Blog: A win for the data protection of UK consumers", ICO, 14 March 2018, <ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/03/blog-a-win-for-the-data-protection-of-uk-consumers/>.

116. There is abundant case law on how to deal with fines for a breach of the EU cartel prohibition and a national prohibition of the same behaviour: *ne bis in idem* does not apply, but fines have to be proportionate. See Case C-617/17, *Powszechny Zakład Ubezpieczeń na Życie S.A.* v. *Prezes Urzędu Ochrony Konkurencji i Konsumentów,* EU:C:2019:283.

interest.[117] This means that even if the offender and the facts are the same, but the interests protected by two different sets of rules differ, the conditions for *ne bis in idem* are not met.[118] This is already the case with the enforcement of national and EU competition law against the same offender with the same facts, let alone kaleidoscopic enforcement of competition, consumer and data protection law that all three pursue a different goal, despite the aforementioned interaction and overlap between their goals.

Besides the *ne bis in idem principle,* the principle governing concurrent offences is codified in the national criminal laws of some of the Member States, to prevent double punishment for the same facts.[119] The ECJ was confronted with this principle in the *Marine Harvest* case on gun-jumping under EU Merger Control.[120] The ECJ did not affirm whether the principle governing concurrent offences is also a general principle of EU law; it addressed the question whether one of the offences[121] is more serious than the other, a condition for the principle of concurrent offences to apply in the first place. The ECJ held that "the EU legislature has not defined one offence as being more serious than the other"[122] and that those provisions "pursue autonomous objectives".[123] In our view, this analysis is also true for the GDPR, consumer, and competition law and the principle governing concurrent offences can therefore not prevent double or even triple penalties in the event of kaleidoscopic enforcement.

Over-enforcement could be especially damaging to SMEs, who have neither the financial nor human resources to navigate the intricate regulatory frameworks which govern the collection and use of data, and protect their

117. Joined Cases C-204, 205, 211, 213, 217 & 219/00, *Aalborg Portland A/S and Others* v. *European Commission*, EU:C:2004:6, para 338. See further van Bockel, *The Ne Bis In Idem Principle in EU Law* (Kluwer Law International, 2010) and our more detailed analysis of double jeopardy in relation to kaleidoscopic enforcement: Yakovleva, Geursen, Arnbak, "Drie mogelijke boetes van mededingings-, consumenten- en persoonsgegevensautoreiten voor hetzelfde datagebraik", (2020) *Tijdschrift Medeclingingsrecht in de Praktijk*, p. 30, nr. 164.

118. Case 14/68, *Walt Wilhelm and Others* v. *Bundeskartellamt*, EU:C:1969:4, para 11.

119. In the event two offences are committed by the same person and by the facts, and one of the offences is more serious than the other, whilst the lesser offence is included in the more serious, the principle bars double punishment and only the more serious offence will be punished.

120. C-10/18, *Mowi ASA (formerly Marine Harvest ASA)* v. *Commission*, EU:C:2020:149.

121. In the case of Marine Harvest, not notifying a concentration to the Commission, in breach of Art. 4(1) of Regulation 139/2004, and executing the concentration before approval by the Commission, in breach of the standstill obligation in Art. 7(1) of Regulation 139/2004.

122. Case C-10/18, *Mowi*, para 99; the ECJ had come to the same conclusion and indicated that "the simultaneous infringement of distinct legal provisions constitutes a notional concurrence"; Case T-704/14, *Marine Harvest ASA* v. *Commission*, EU:T:2017:753, para 372. Marine Harvest had not invoked the principle of notional concurrence, but only the principle of concurrent offences.

123. Case C-10/18, *Mowi*, para 103.

interests in dealings with enforcement authorities.[124] The risk of over-enforcement itself could deter those companies from engaging in certain data protection practices, which would weaken their market position *vis-à-vis* the big tech companies and, as a result, strengthen the market power of the latter.

The commercial success of companies by their use of data, as well as the benefits for consumers (better products and services), can be cancelled out by the incorrect or excessively restrictive enforcement of the rules. Over-enforcement due to lack of coordination, and the risk of confronting overlapping enforcement by three different authorities (kaleidoscopic enforcement) could also reduce the competitiveness of European companies in the global market.[125]

4. Addressing the drawbacks of kaleidoscopic enforcement

In this section, we discuss how risks under kaleidoscopic enforcement can be mitigated and why a different approach is needed, and we suggest an institutional solution.

The drawbacks of kaleidoscopic enforcement are mostly due to the compartmentalized structure of enforcement for each of the competition, consumer, and personal data protection authorities, which still largely operate in silos. Let us look at two examples to explain this point. In example one, an inebriated driver is speeding, proceeds to run a red light and causes an accident. The driver will likely be prosecuted by only one authority (the public prosecutor), even though the driver has violated several norms and laws with one sole action. There is likely to be only one sanction, which looks at the seriousness of the breach by reviewing all broken norms in one go under the criminal law principles of concurrent offences and/or notional concurrence. In example two, a dominant company collects and uses the personal data of existing customers, without their consent, to offer new and unrelated services. This single use by the company of the customer database can – at the same time – be: (1) a breach of the GDPR, due to lack of consent; (2) unfair use of the data under consumer protection law;[126] and (3) an abuse of dominance under competition law, since competitors on the market for the new service do

124. See Commission Communication, "Long term action plan for better implementation and enforcement of single market rules", COM(2020)94 final, p. 2.

125. See Hackenbroich, "Reality bytes: Europe's bid for digital sovereignty", European Council on Foreign Relations, 17 Oct. 2018, <www.ecfr.eu/article/commentary_reality_bytes_europes_bid_for_digital_sovereignty>.

126. The Italian Consumer Authority imposed fines totalling EUR 900,000 on three energy companies for using their customer database for the unsolicited supply of services to

not have access to the same data.[127] The company can then face three separate enforcement procedures by two or three authorities, each imposing its own sanctions.

We contend that to address the drawbacks of kaleidoscopic enforcement, discussed in section 3 above, an institutional solution is necessary to overcome the compartmentalized structure of competition, consumer, and data protection enforcement. Without such an institutional mechanism, the effectiveness of attempts to ensure consistency of data-related enforcement under competition, consumer, and data protection law would be limited. Several scholars have suggested that the coherent application of the three areas of law could be built upon the principle of fairness, which is common to all of them.[128] However, although – as an open norm – "fairness" does provide for the flexible interpretation of legal norms, including the possibility of borrowing concepts from other areas of law for purposes of interpretation, this concept *by itself* does not bind enforcement authorities to do so in a consistent manner. Hesselink rightly argues that although fairness is a principle in most areas of law, "[t]here is no inner coherence between so-called good faith rules and doctrines".[129] Fairness serves a different purpose in each area of law – the one which that area of law aims to achieve. Therefore, depending on the normative value structure of a particular area of law, it could be both viewed as a value in itself or one of the factors in the function of welfare.[130]

Mechanisms adopted to resolve problems similar to kaleidoscopic enforcement in the context of decentralized enforcement[131] and parallel public and private enforcement[132] in other areas of law, such as competition law, are

consumers. This was considered unfair commercial practice under consumer protection law (Decisions PS10998, PS11140 and PS11172 of 24 Oct. 2018, *Autorità Garante della Concorrenza e del Mercato*).

127. The French Competition Authority imposed a 100 million euro fine on gas and electricity company Engie for illegal abuse of dominance when it used its historical data file of customers on regulated gas tariffs to offer those customers new market-based contracts for gas and electricity, whereas their competitors on that market, which had just been opened up to competition, did not have access to that database (Decision 17-D-06 of 21 March 2017, *Autorité de la concurrence*).

128. EDPS Opinion 8/2016, cited *supra* note 15, p. 8; Graef, Clifford and Valcke, op. cit. *supra* note 15, 202–203, 223; Kalimo and Majcher, op. cit. *supra* note 76, 233.

129. Hesselink, "The concept of good faith" in Hartkamp et al. (Eds.), *Towards a European civil code* – 4th rev. and exp. ed. (Kluwer Law International, 2011), pp. 619–649.

130. Kaplow and Shavell, "Fairness versus welfare", 114 *Harvard Law Review* (2001), 1011–1017.

131. Since Regulation 1/2003 on the implementation of the rules on competition (O.J. 2003, L 1/1) came into force, national competition authorities are competent to apply Arts. 101 and 102 TFEU, as well as the Commission. Given their direct effect, those provisions could already be applied by national courts.

132. See Jones, op. cit. *supra* note 16.

also of limited relevance. When it comes to public enforcement by two national competition authorities in the same case, one of them may suspend or even terminate the case.[133] When a national court has to decide on Articles 101 and 102 TFEU, the Commission and national competition authorities may intervene as an *amicus curiae*, also on their own initiative.[134] According to the *Masterfoods* doctrine, since there is a certain hierarchy in the enforcement of EU competition law, national courts and competition authorities may not "take decisions which would run counter to the decision adopted by the Commission".[135] With respect to private enforcement of competition law, the national court deciding on a damages claim is bound by a decision taken by the Commission.[136] The Damages Directive[137] has introduced mechanisms of proof which ensure coherence as well. The national judge is bound by a final decision of a national competition authority of the same Member State;[138] a decision of a national competition authority of another Member State has at least the status of *prima facie* evidence.[139] In *Skanska*, the principle of effectiveness as applied by the ECJ even led to convergence in the interpretation of which company can be held responsible to pay the fine under public enforcement and the damage under private enforcement.[140] In contrast to decentralized and public-private enforcement of competition law, there is no hierarchy between competition, consumer and data protection law when it comes to kaleidoscopic enforcement. Therefore, the *Masterfoods* doctrine cannot serve as a way to ensure coherence of enforcement in these three areas of law.

The convergence which the ECJ established in *Skanska* by breaking the wall between the two enforcement silos of public and private enforcement, might perhaps be used as an ultimate remedy to create coherence in kaleidoscopic enforcement, but does not offer an up-front solution to the problems of kaleidoscopic enforcement. The *amicus curiae* procedure can, however, serve as one of the tools to achieve such coherence by allowing

133. Art. 13(1) Regulation 1/2003.

134. Art. 15(3) Regulation 1/2003.

135. Art. 16 Regulation 1/2003; this provision and the hierarchy which it reflects, stems from Case C-344/98, *Masterfoods* v. *HB Ice Cream,* EU:C:2000:689, paras. 51–52. The other way around, the Commission is not bound by a decision of a national court (para 48).

136. Already on the basis of Art. 16 Regulation 1/2003; the Damages Directive did not change that.

137. Directive 2014/104 on actions for damages under national law for infringements of competition law, O.J. 2014, L 349/1.

138. The infringement is deemed to be irrefutable under Art. 9(1) Damages Directive.

139. Art. 9(2) Damages Directive.

140. Case C-724/17, *Vantaan kaupunki* v. *Skanska Industrial Solutions Oy and Others*, EU:C:2019:204; cf. Wurmnest, "Liability of 'undertakings' in damages actions for breach of Articles 101, 102 TFEU: *Skanska*", 57 CML Rev. (2020), 915–934.

authorities from the different domains of law to become each other's "friends" by giving an opinion in each other's cases. For example, DPAs could give their opinion to competition authorities in data-driven mergers. On the other hand, although this approach would allow authorities to learn from each other and may eventually lead to more coherent enforcement, the downside of it is the non-binding nature of *amicus curiae* briefs. The other mechanism of suspension or closure of cases which are already subject to an investigation by another authority could mitigate the risks of over-enforcement. Rules and mechanisms to operationalize such suspension or closure could be a part of the institutional mechanism proposed below.

In determining the design of the institutional solution to kaleidoscopic enforcement, an important question to answer is whether "enforcement silos" should be "broken" completely or only to a certain degree.

An illustration of how enforcement silos could be broken down appears in the 2019 article by Giovanni Buttarelli, the European Data Protection Supervisor (EDPS). In that article, he noted that the German competition authority's enforcement action against Facebook "could give some hints for future reflection on a possible unique regulator, responsible for digital markets".[141] Indeed, competition and consumer authorities in several countries already have been fully (the Netherlands, Poland and France) or partially (Italy and Hungary) integrated into one enforcement authority.[142] However, we have three reservations with the idea of breaking down the silos between competition and consumer authorities on the one hand, and data protection authorities on the other hand.

First, there is an ontological problem with integrating competition and consumer authorities with data protection authorities, as exemplified by the diverging *individual rights* nature of personal data protection and *economic* nature of competition and consumer protection. The ideology (or discourse) governing the creation and content of rules contained in a specific area of law inevitably affects the ethos of the enforcement mechanism established to ensure those rules are complied with.[143] Although it would be desirable to enhance coordination between the authorities, completely dismantling the

141. Buttarelli, "This is not an article on data protection and competition law", *CPI Antitrust Chronicle* (Feb. 2019), <edps.europa.eu/sites/edp/files/publication/19-03-11_cpi_buttarelli_en.pdf>.

142. For a comprehensive overview, see Cseres, "Integrate or separate: Institutional design for the enforcement of competition law and consumer law", Amsterdam Law School Legal Studies Research Paper No. 2013-03, <papers.ssrn.com/sol3/papers.cfm?abstract_id=2200908>.

143. There is ample literature showing how the discourse governing the formation of the WTO Agreement has affected the ethos of the WTO Adjudicating bodies. For a discussion, see Yakovleva op. cit. *supra* note 37, 507–515.

silos could undermine the heightened level afforded to individual rights for the protection of personal data guaranteed by the EU Charter.[144]

Second, the idea of a single EU-level digital regulator would be difficult to realize for political reasons. For such a regulator to be able to be effective, the transferring of essential regulatory and enforcement powers from national enforcement authorities would be necessary. If the negotiation history in the EU Council surrounding the GDPR provisions (in terms of the one-stop-shop and consistency mechanisms) are anything to go by, national DPAs are reluctant to give up their powers in favour of an EU body and are strongly opposed to the creation of a fully-fledged EU-level data protection regulator.[145]

Third, there is currently no EU-level consumer authority. Forming one would be difficult for political and economic reasons, as explained in the previous paragraph. The diversity of EU Member States' approaches to enforcing consumer law would further complicate the issue.[146] As a result, the EU is unlikely to pass EU legislation aiming to introduce an effective EU-level digital regulator.

In sum, the institutional solution to kaleidoscopic enforcement should not, for the reasons described above, completely dismantle the silos between competition, consumer, and data protection laws. It should, however, ensure the interoperability between the three enforcement systems.

Another possible institutional solution to kaleidoscopic enforcement is the Digital Clearing House – launched by the EDPS in 2016[147] – a voluntary coordination mechanism between competition, consumer, and data protection authorities. The aim of the Clearing House is for different supervisory authorities to share information and collaborate, within the boundaries of legal competences and while respecting confidentiality.[148] The Digital Clearing House discusses (but does not allocate) the most appropriate legal regime for pursuing specific cases or complaints related to services online (especially for cross-border cases where there is a possible violation of more than one legal framework), and identifying potential coordinated actions or awareness initiatives at European level which could stop or deter harmful

144. For a discussion of how the normative rationale underlying the protection of personal data protection affects the optimal level of such protection, see Yakovleva, op. cit. *supra* note 37, 455–464.

145. For discussion, see Jančūtė, "European data protection board: A nascent EU agency or an 'intergovernmental club'?", 10 *International Data Privacy Law* (2019), 57–75.

146. Faure and Weber, op. cit. *supra* note 48.

147. EDPS Opinion 8/2016, cited *supra* note 15, pp. 3, 15. See also NAIH, "Resolution on new frameworks of cooperation", Budapest Spring Conference, 27 May 2016, <www.naih.hu/budapest-springconf/files/Resolution – new-frameworks.pdf>.

148. Ibid.

practices.[149] In several meetings, participants explored institutionalized cooperation mechanisms and information-sharing protocols between regulatory authorities, as well as between the networks of such authorities.[150] To date, however, no coordinated enforcement actions have been taken or planned. Although the number of participants at Clearing House meetings has been steadily growing,[151] as of 2018 they still represent only about one third of all Member States' competition, consumer, and data protection authorities. This is unsurprising given its voluntary nature. Thus, although the Digital Clearing House is a good start for cooperation, as a discussion forum, it is not enough to overcome the pitfalls of kaleidoscopic enforcement throughout the EU. What is needed is a binding, pan-European coordination mechanism which operates under a more formalized structure.

Competition, consumer, and data protection authorities at the EU Member State level have been gradually recognizing the need for intra-disciplinary cooperation protocols – typically bilateral.[152] These cooperation mechanisms, however, are limited to enforcement within a particular Member State. The problem is that the procedures, level of cooperation and the division of tasks between authorities in each Member State could differ, which would prevent a bottom-up formation of intra-disciplinary coordination at EU level.

For these reasons, we argue that the most effective way to overcome the drawbacks of kaleidoscopic enforcement when enforcing against data-related practices is to establish a mandatory coordination mechanism at the EU level between competition, consumer, and personal data protection authorities. For the mechanism to have a firm legal basis – one of the conditions for effective

149. EDPS Opinion 8/2016, cited *supra* note 15, p. 15.

150. Statement from the second meeting of the Digital Clearinghouse, <edps.europa.eu/sites/edp/files/publication/17-11-30_statement_2nd_meeting_dch_en.pdf>; Statement from the fourth meeting of the Digital Clearinghouse, <edps.europa.eu/sites/edp/files/publication/18-12-10_4th_dch_statement_en.pdf>.

151. The number grew from 20 enforcement authorities in 2017 to over 30 in 2018. See the Statements from the second and fourth meetings, ibid. The most recent statements from the Digital Clearing House meetings no longer mention the number of attendees.

152. E.g. the Dutch DPA has cooperation protocols with authorities at the national level on the division of tasks in overlapping areas of supervision: Dutch Media Authority, the Central Bank of the Netherlands, Dutch Health Care Inspectorate, Dutch Authority for Consumers & Markets, Dutch Healthcare Authority, Inspectorate for Education, Inspectorate for Identifying Data, and Telecommunications Agency. See <autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/nationale-samenwerking>. In a similar vein, the French DPA has published a note on "new regulation methods concerning data" jointly with other authorities, including the French Competition Authority, Financial Markets Authority, Railway Authority, Electronic and Postal Communications Authority, Energy Regulation Commission and Media Council. See <www.cnil.fr/fr/cooperations-entre-regulateurs>.

cooperation[153] – it should be introduced by EU legislation determining the design of the coordination mechanism and the procedural aspects of coordination.[154] The coordination mechanism could use, as a prototype, the existing pan-European coordination mechanisms of consumer or competition authorities, discussed above (section 3.1), as there is no need to reinvent the wheel. An advantage of doing so is that it would reduce the transaction costs of designing the mechanism and of adjusting to the mechanism by all participating authorities, as at least one-third of them – competition or consumer ones – would already be familiar with the way it works.[155]

Creating this type of coordination mechanism should form part of the EU's current efforts to improve consistency in the enforcement of EU rules in the internal market. For example, in its White Paper on Artificial Intelligence, the European Commission proposes creating a European governance structure on AI in the form of a framework for the cooperation of national enforcement authorities.[156] The Commission states that this governance structure could, in particular, serve as a forum for exchanging information and best practices, advising on standardization activity and certification, and playing a role in facilitating the implementation of the legal framework on AI.[157] The EDPS supports the Commission's proposal and recommends, in particular, that any new regulatory framework for AI should avoid overlap of different supervisory authorities and include a cooperation mechanism.[158] In parallel, as part of the new Industrial Strategy for Europe, the Commission has adopted a Single Market Enforcement Action Plan, which proposes concrete steps on strengthening joint efforts to ensure the consistent implementation and enforcement of EU rules across the internal market, including the Single Market Enforcement Task Force.[159] The Action Plan's measures aim to reduce regulatory and administrative barriers to single market cross-border

153. Kloza and Moscibroda, "Making the case for enhanced enforcement cooperation between data protection authorities: Insights from competition law", 4 *International Data Privacy Law* (2014), 135.

154. Because each of these areas of law, as mentioned in section 3.2 *supra*, has the (shared) goal of achieving the internal market, the EU has competence to adopt this legislative instrument under Art. 26 TFEU.

155. Building on the experience of EU-wide coordination of competition authorities, Kloza and Moscibroda have already formulated a set of conditions for an effective coordination mechanism. Kloza and Moscibroda, op. cit. *supra* note 153, 135.

156. COM(2020)65 final, cited *supra* note 6, p. 24.

157. Ibid.

158. Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust, 29 June 2020 <edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf>.

159. Commission Communication, "A New Industrial Strategy for Europe", COM(2020)102 final, pp. 5–6; Commission Communication, cited *supra* note 124, p. 4.

trade, and facilitate the circulation of goods and services.[160] None of these documents devote any attention to the current incoherence of competition, consumer, and data protection enforcement in data-related cases.

5. Conclusion

Ever since EU Commissioner Kuneva's much-cited 2009 quote – that personal data has become the oil and currency of the digital world – it has become clear that access to huge amounts of data and the ability to collect it have become critical for achieving commercial success in the 21st century. A healthy information economy requires clear rules and effective supervision that do justice to the interrelated policy objectives of privacy, consumer protection, and competition. As competent authorities in the three areas of law intensify their enforcement efforts against data-related practices, the drawbacks of kaleidoscopic enforcement demonstrated in this article will become increasingly manifest over time. A binding pan-European coordination mechanism between competition, consumer, and data protection authorities is needed to ensure coherent enforcement of data-related rules in each legal domain. Now that the European Commission has initiated a wide range of measures to ensure the coherence of implementation and enforcement of EU rules, it is the right time to create this mechanism and include it in the EU agenda for the next four years.

160. For an overview of barriers, see Commission Communication, "Identifying and addressing barriers to the Single Market", COM(2020)93 final.