Max Planck Institute
for Innovation and Competition

Max Planck Institute for Innovation and Competition Research Paper No. 18-08

Marco Botta and Klaus Wiedemann

EU Competition Law Enforcement vis-à-vis Exploitative Conducts in the Data Economy
Exploring the Terra Incognita

Max Planck Institute for Innovation and Competition Research Paper Series

EU Competition Law Enforcement vis-à-vis Exploitative Conducts in the Data Economy

Exploring the Terra Incognita

Marco Botta[1] *and Klaus Wiedemann*[2]

WORKING PAPER

[1] Senior Research Fellow, Max Planck Institute for Innovation and Competition, Munich (Germany). E-Mail: marco.botta@ip.mpg.de.
[2] Junior Research Fellow, Max Planck Institute for Innovation and Competition, Munich (Germany). E-Mail: klaus.wiedemann@ip.mpg.de.

Table of contents

1. Introduction

In the XV and XVI century the expression *terra incognita* was used in cartography to indicate the "unknown lands" of the globe. For centuries, the Portuguese and Spanish explorers sailed to the west, looking for a shorter way towards the East Indies. In organizing their expeditions, they could not rely on detailed maps; they rather relied on anecdotes from other sailors, the movements of the stars and ultimately the experience previously gained in sailing in safe and well-known seas.

Nowadays, our *terra incognita* is represented by the data economy. The past decade has witnessed the rapid proliferation of new business models that mainly rely on the processing of large amounts of users' data, commonly known as "Big Data".[3] The data-driven economy has generated a substantial number of innovations both in terms of new products that benefit consumers, as well as new organization and marketing strategies that increase the firms' productivity.[4] On the other hand, the large amount of data controlled by a limited number of online platforms has generated a number of competition law concerns. A clear "map" still does not exist in this area and, thus, a pending question is whether and to what extent the traditional competition law principles can be transferred from the "real" to the data economy. To this regard, while enforcers have mainly focused their attention on exclusionary practices carried out by online platforms to the detriment of their competitors (e.g. the recent EU Commission decision in the *Google Shopping* case[5]), in this paper

[3] According to Laney, Big Data differ from traditional datasets due to the so-called "3 Vs": larger "volume", larger "variety" of the information collected and "velocity" in which data are processed thanks to the exponential growth of computing power. In particular, data analytics is becoming more and more automated task. This development is accompanied by the increasing use of software relying on self-learning algorithms and systems using artificial intelligence. Secondly, in the coming years data will be collected not only on the Internet, but also by an increasing number of sensors installed in electronic devices that interact with each other (i.e. Internet of Things, IoT). Therefore, the advent of IoT will increase the number of industrial manufacturers and service providers that collect, process and transfer a large amount of data via their devices.
Laney D., *3D Data Management: Controlling Data Volume, Velocity and Variety*. Meta Group (Gartners Blog post), posted on 6.2.2001. Available at http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf (22.5.2018).

[4] OECD Secretariat, *Data-Driven Innovation. Big Data for Growth and Well-Being*. Report published on 6.10.2015, p. 26. The text is available at: http://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm (22.5.2018).

[5] Commission Decision of 27.6.2017 relating to proceedings under Art. 102 TFEU and Art. 54 Agreement on the European Economic Area. AT.39740 – *Google Search (Shopping).* The text of the decision is available at: http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39740 (22.5.2018).

we "explore" exploitative abuses in the data economy. In particular, we focus on the enforcement challenges faced by the EU Commission/National Competition Authorities (NCAs) to sanction exploitative conducts in data markets and potential remedies, while we skip the issues of relevant market definition and market power; subjects that have already been discussed at length in the literature. [6]

Exploitative conducts are unilateral behaviours that distort competition by directly harming final consumers/customers, rather than excluding competitors. The imposition of excessive and discriminatory prices and the unilateral imposition of unfair contractual clauses are examples of exploitative conducts that could harm either direct customers or final consumers. In the USA, after the ruling of the US Supreme Court in *Trinko*, it is clear that the Sherman Act sanctions only exclusionary conducts that harm competitors, rather than exploitative abuses.[7] The latter practices are rather prosecuted in the context of the consumer law framework: the Federal Trade Commission (FTC) has a well-established experience in investigating discriminatory pricing and unfair contractual clauses under Section 5 FTC Act.[8] In Europe, on the contrary, Art. 102 Treaty

[6] In particular, a number of authors have focused their attention to the application of the concept of multi-sided markets, initially developed by Tirole, to online platforms. Secondly, a number of articles have discussed whether and to what extent the accumulation of large amount of data (i.e. big data) by online platforms may represent an entry barrier in the market.
See for instance:
Rubinfeld D., Gal M. (2017), "Access Barriers to Big Data" 59 *Arizona Law Review:* 339.
Schepp N. P., Wambach A. (2016), "On Big Data and Its Relevance for Market Power Assessment" 7(2) *Journal of European Competition Law and Practice*: 120.
Graef I. (2015), "Market Definition and Market Power in Data: the Case of Online Platforms" 38(4) *World Competition:* 473.
Filistrucchi L., Gerardin D., Van Damme E. (2013), "Identifying Two-Sided Markets" 36(1) *World Competition*: 33.
Lianos I., Motchenkova E. (2013), "Market Dominance and Search Quality in the Search Engine Market" 9(2) *Journal of Competition Law and Economics*: 419.
Rochet J. C., Tirole J. (2013), "Two-Sided Markets: A Progress Report" 37(3) *RAND Journal of Economics*: 645.

[7] In *Trinko*, the US Supreme Court stated that "The mere possession of monopoly power, and the concomitant opportunity to charge monopoly prices, is not only not unlawful; it is an important element of the free-market system. The opportunity to charge monopoly prices – at least for a short period – is what attracts business acumen in the first place."
US Supreme Court, *Verizon Communications Inc v. Trinko*. Ruled on 13 January 2004.
For a comparison of the EU and US approach to sanction exploitative conducts under competition rules, see Gal, M. (2004), "Monopoly Pricing as an Antitrust Offense in the US and the EC: Two Systems of Belief About Monopoly?" 49 *Antitrust Bulletin:* 343-384.

[8] Section 5(a) provides the FTC the power to prosecute "unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce"
Federal Trade Commission Act, 15 U.S.C. §§ 41-58, as amended.

of the Functioning of the European Union (TFEU) lists a number of exploitative conducts as examples of abuses of dominant position.[9] In particular, by studying the *travaux préparatoires* of the Rome Treaty, Akman has concluded that the initial intention of the EU founding fathers was to sanction via Art. 102 TFEU primarily exploitative conducts, rather than exclusionary practices.[10] Nevertheless, due to the high burden of proof and concerns over the risk of market regulation, the EU Commission has seldom investigated this type of abuses under Art. 102 TFEU.[11] This situation has progressively changed over the recent years, when NCAs from a number of EU Member States have sanctioned cases of excessive pricing and unfair contractual clauses in network industries recently liberalized; industries characterized by high entry barriers, where the regulatory framework cannot effectively tackle such structural competitive issues.[12] The question explored in this paper is whether the increasing enforcement of EU competition law *vis-à-vis* exploitative conducts will also have an impact on data markets in the long term.

The paper is structured as follows: after an overview of the CJEU case law *vis-à-vis* exploitative abuses (i.e. our "safe sea"), we start the exploration of the *terra incognita* by discussing in section 3

For a detailed analysis of the enforcement of Section 5 by the FTC in the area of privacy protection and big data, see:
- Solove D., Hartzog W. (2014), "The FTC and the New Common Law of Privacy" 114 *Columbia Law Review:* 583.
- Tene O., Polonetsky J. (2013), "Big Data for All; Privacy and User Control in the Age of Analytics" 11(5) *Northwestern Journal of Technology and Intellectual Property:* 239.

[9] Consolidated version of the Treaty on the Functioning of the European Union. OJ C-326, 26.10.2012, p. 47-390.

[10] Akman P. (2009), "Searching for the Long-Lost Soul of Article 82 EC" 29(2) *Oxford Journal of Legal Studies:* 267-303.

[11] The Commission has adopted only four decisions sanctioning excessive prices: 1) Case *General Motors*, decision of 19/12/1974, OJ L 29/14; 2) Case *United Brands*, decision of 17/12/1975, OJ L 95/1; 3) Case *British Leyland*, decision 84/379/ECC of 2/7/1984, OJ L 207/11; 4) Case *Deutsche Post II*, decision of 25/7/2001, OJ L 331/40. With the exceptions of *British Leyland*, these decisions have been annulled by the CJEU or the General Court (GC).

[12] In relation to the increased tendency by a number of NCAs in Europe to sanction exploitative abuses of dominance, see:
- Karova R., Botta M. (2017), "Sanctioning Excessive Energy Prices as Abuse of Dominance; Are the EU Commission and the National Competition Authorities on the Same Frequency?" in Parcu P. L., Monti G., Botta M. (eds.), *Abuse of Dominance in EU Competition Law: Emerging Trends* (Edward Elgar Publisher).
- Svetlicinii A., Botta M. (2015), "Enforcement of Competition Rules in Regulated Industries: Abuse of Dominance Practices in the New EU Member States, Candidate Countries and Potential Candidates" in Di Porto F., Drexl J. (eds.), *Competition Law as Regulation*? Cheltenham, Edward Elgar Publisher**:** 276-305.
- Svetlicinii A., Botta M. (2012), "Article 102 TFEU as a Tool of Market Regulation: 'Excessive Enforcement' Against 'Excessive Prices' in the New EU Member States and Candidate Countries" 8(3) *European Competition Journal*: 473-496.

the role of EU competition law intervention in the data economy from a general point of view. Afterwards, in section 4 we analyse three categories of abuses that may harm consumers/customers in data markets:

- Unfair prices: in data markets, this conduct could take the form of either an "excessive" amount of personal data that online platforms request final consumers to provide in order to get "free" access to an online service.[13] Alternatively, the holder of an essential dataset could impose an excessive access price on industrial customers to get access to its database.[14]

- Discriminatory pricing: via an analysis of personal data and by means of predictive modelling (i.e. profiling), algorithms facilitate cases of price discrimination among different consumers who purchase goods and services from a dominant online platform.

- Unfair contractual clauses: by unilaterally imposing a change of the data protection terms/privacy policies, a dominant online platform could decrease the product quality of an online service. In other words, the final consumer would receive the same online service by "paying" a higher price in terms of lower privacy standards.

Our journey in the *terra incognita* ends – hopefully safely – with a discussion of the types of competition law remedies that could address the harms analysed in section 4. In terms of remedies, the paper looks at the role of fines and behavioural remedies to sanction exploitative conducts in data markets. In particular, the paper explores the possibility that the NCA may borrow from the European data protection regime a number of behavioural remedies to tackle forms of privacy degradations unilaterally imposed by online platforms. In

[13] The expression online "free" service is generally considered misleading for consumers. The online service delivered, in fact, "…involve non-pecuniary costs (for consumers) in the form of providing personal data, paying attention to ads, or the opportunity costs of reading privacy policies."
OECD Secretariat, *Big Data: Bringing Competition Policy to the Digital Era.* Report published on 27.10.2016, DAF/COMP(2016)14, p. 25, available at: http://www.oecd.org/daf/competition/big-data-bringing-competition-policy-to-the-digital-era.htm (22.5.2018).

[14] On the more general discussion whether and under what conditions access rights to data should be implemented, see Drexl J., Hilty R. M. et al., "Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's 'Public consultation on Building the European Data Economy'", available at
http://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Statement_Public_consultation_on_Building_the_EU_Data_Eco_28042017.pdf (22.5.2018).

other words, the question is whether the rights provided in the EU General Data Protection Regulation (GDPR)[15] to natural persons, such as transparency obligations regarding the treatment of personal data, opt-in and opt-out rights for data subjects, access rights and data portability rights might be either imposed or negotiated by the NCA as a behavioural remedy in the context of a competition law investigation.

The paper is timely, since it looks at the recent EU Commission decision in the *Facebook-WhatsApp* merger.[16] Also, the paper discusses the on-going investigations conducted by the German Competition Authority (*Bundeskartellamt*) in the *Facebook* case.[17] Finally, the paper is timely in view of the entry into force of the GDPR in May 2018. This Regulation aims to strengthen and unify the privacy enforcement tools in Europe, and thus raises the question of whether EU competition law still has any role to play to prevent exploitative abuses that affect the personal data of final consumers.

2. Exploitative conducts under EU competition law – the CJEU case law

As mentioned in the previous section, Art. 102 TFEU lists a number of exploitative conducts as possible abuses of dominance, such as: "directly or indirectly imposing unfair purchase or selling prices" (i.e. excessive prices),[18] "applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage" (i.e. discriminatory pricing)[19] and "making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such

[15] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L-119, 4.5.2016, p. 1-88.

[16] After the 2014 approval of the acquisition of WhatsApp by Facebook without the imposition of any condition, in 2017 the EU Commission imposed a fine for having integrated WhatsApp and Facebook users' databases without having properly informed the EU Commission about such choice. The merging parties were thus fined for having provided misleading and wrong information to the EU Commission during the 2014 review of the concentration that affected the merger assessment.
EU Commission decision in Facebook/WhatsApp adopted on 17.5.2017. Case M. 8228.

[17] https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html;jsessionid=3249A6E0B9D32CC0F0ED795044CA4128.1_cid387?nn=3591568 (22.5.2018).

[18] Art. 102(a) TFEU.

[19] Art. 102(c) TFEU.

contracts" (i.e. unfair contractual clauses).[20] Nevertheless, for a long period of time the EU Commission has primarily sanctioned exclusionary, rather than exploitative abuses. Therefore, it is not surprising that the CJEU case law in this area is rather limited. This section aims at analysing the case law of the EU Court of Justice *vis-à-vis* excessive and discriminatory pricing as well as unfair contractual clauses, in order to find some guidance for the exploration of our *terra incognita* in the following sections.

2.1. CJEU case law on excessive pricing: the long journey from *United Brands* to *Latvian Copyright Society*

In *General Motors,* the CJEU recognized for the first time the possibility for the EU Commission to sanction excessive pricing under Article 102 TFEU.[21] However, in that judgement the Luxembourg Court did not clarify when the price imposed by a dominant undertaking should be considered excessive. The CJEU ruled that "an undertaking in a dominant position may abuse its dominant position by imposing a price which is excessive in relation to the economic value of the service provided…"[22] In *United Brands,* the CJEU confirmed that prices are excessive when they have "…no reasonable relation to the economic value of the product….",[23] but it failed to provide guidance on how the EU Commission should quantify the economic value of the product. In the land-mark ruling, the EU Commission put forward as main evidence of "unfairness" the fact that the price of Chiquita bananas sold by United Brands in Germany, Denmark, the Netherlands and the Benelux countries was on average 100% higher than in Ireland,[24] although there were no substantial differences in terms of transportation costs and quality of the product. The Court, however, rejected the evidence put forward by the EU Commission: the EU Commission should have analysed the cost structure of the dominant undertaking and compare the production costs with the wholesale price of bananas, in order to verify whether the profit margin of the dominant company was "excessive".[25]

Over the years, the CJEU has reiterated the *United Brands* cost-price test in a number of preliminary rulings requested by the national courts.[26] However, these judgements often had a "declaratory nature":

[20] Art. 102(d) TFEU.
[21] Case 26/75, *General Motors Continental v. Commission* (1975) ECLI:EU:C:1975:150.
[22] *Ibid.,* para. 11-12.
[23] Case 27/6, *United Brands Company v. Commission* (1976) ECLI:EU:C:1978:22, para. 250.
[24] *Ibid.,* para. 239.
[25] *Ibid.,* para. 251-252.
[26] See, for instance:

the CJEU re-stated the *United Brands* test, but it left to the referring court the duty to apply the test to the facts of the individual case.[27] The EU Commission, on the other hand, rarely investigated this type of abuses. [28] As recognized by the Court in *United Brands*, in fact, the analysis of the production costs may be extremely complex, in particular in relation to the estimation and allocation of fixed costs. Secondly, besides being difficult to apply, the cost-profit test would require the EU Commission to assess the degree of profitability of the incumbent firm, an assessment that would be almost equivalent to a form of price regulation.[29] Finally, the cost-profit test did not take into consideration the demand fluctuations; as noticed by the European Commission in *Scandlines,* "…customers are notably willing to pay more for something specific attached to the product/service that they consider valuable".[30]

The Court of Justice has recently acknowledged the difficulties behind the application of the *United Brands* cost-price test in its ruling in *Latvian Copyright Society.*[31] The case concerned the excessive rates that the collective society of Latvian copyright holders requested for the use of musical works. According to the Latvian Competition Authority, the royalty rates were excessive, since they were between 50% and 100% higher than the rates requested in other EU Member

- Case 30/87, *Corinne Bodson v SA Pompes Funèbres des Régions Libérées* (1988) ECLI:EU:C:1988:225.
- Case 66/86, *Ahmed Saeed Flugreisen and Silver Line Reisebüro GmbH v Zentrale zur Bekämpfung unlauteren Wettbewerbs e.V* (1989) ECLI:EU:C:1989:140.
- Case C-323/93, *Société Civile Agricole du Centre d'Insémination de la Crespelle v Coopérative d'Elevage et d'Insémination Artificielle du Département de la Mayenne* (1994) ECLI:EU:C:1994:368.

[27] Wahl N., "Exploitative High Prices and European Competition Law – a Personal Reflection." in Konkurrensverket (Swedish Competition Authority, ed.), *The Pros and Cons of High Prices* (Stockholm, Lenanders Grafika, 2007), p. 54.
The paper is available at:
http://www.kkv.se/upload/filer/trycksaker/rapporter/pros&cons/rap_pros_and_cons_high_prices.pdf (22.5.2018),

[28] The Commission has adopted few decisions sanctioning excessive prices. See in particular:
- Case *General Motors*, decision of 19/12/1974, OJ L 29/14;
- Case *United Brands*, decision of 17/12/1975, OJ L 95/1;
- Case *British Leyland*, decision 84/379/ECC of 2/7/1984, OJ L 207/11;
- Case *Deutsche Post II*, decision of 25/7/2001, OJ L 331/40.

[29] This was the argument put forward by the Court of Appeal of England and Wales in 2007. The Court rejected the cost-profit test proposed by the EU Court of Justice in *United Brands* arguing that "(Article 102 TFEU) is not a general provision for the regulation of prices."
At the Races Limited v. The British Horse Racing Limits and others. England and Wales Court of Appeal (Civil Division), 2007 EWCA Civ 38, para. 217.

[30] *Scandlines Sverige AB v. Port of Helsingborg.* Decision adopted on 23/7/2004, COMP/A.36/568/D3.

[31] Case C-177/16, *Autortiesību un komunicēšanās konsultāciju aģentūra v. Latvijas Autoru apvienība v Konkurences padome* (2017) ECLI:EU:C:2017:689.

States, such as Lithuania and Estonia.[32] Unlike *United Brands*, the Court of Justice did not reject the comparison with other Member States as a way to determine whether the prices charged by the dominant undertaking were unfair. In particular, the Court pointed out that that besides the cost-price test "…there are other methods by which it can be determined whether a price may be excessive."[33] The CJEU ruled that the price comparison with other EU Member States was a "valid" method[34] when the Member States were selected "in accordance with objective, appropriate and verifiable criteria",[35] such as "consumption habits and other economic and sociocultural factors, such as gross domestic product per capita and cultural and historical heritage."[36]

The second issue discussed in *Latvian Copyright Society* concerned the threshold of price unfairness; in other words, when a price is indeed so high that it must be considered excessive. This issue had not been clarified in *United Brands*, where the Court simply ruled that the price was excessive when it was not related to the economic value of the product. In *Latvian Copyright Society*, the Court clarified that "there is no minimum threshold" to determine when the price is excessive.[37] According to the CJEU, a price is unfair if it is "appreciably higher" than it would be under normal market conditions.[38] In particular, if the price difference with other Member States is "significant" and "persistent", it could be considered unfair.[39] Therefore, the price by the dominant company that is occasionally higher in one Member State than in the others would not represent an abuse of dominance: the price difference has to last in time and the difference has to be substantial. Finally, it is up to the dominant company to justify the reasons of the price difference, which could be due to differences in costs structure and demand fluctuations.[40]

At first glance, the CJEU ruling of *Latvian Copyright Society* does not seem particularly innovative: the price comparison with similar/identical products sold in other Member States seems a rather intuitive method to determine if a price is excessive. Such a method had been suggested by Akman and Garrod, and has already been followed by a number of NCAs and national courts before the CJEU ruling.[41] The added value of *Latvian Copyright Society* is that forty

[32] *Ibid.*, para. 9.
[33] *Ibid.*, para. 37.
[34] *Ibid.*, para. 38.
[35] *Ibid.*, para. 41.
[36] *Ibid.*, para. 42.
[37] *Ibid.*, para. 55.
[38] *Ibid.*, para. 55.
[39] *Ibid.*, para. 55.
[40] *Ibid.*, para. 58.
[41] Akman P., Garrod L. (2011), "When Are Excessive Prices Unfair?" 7(2) *Journal of Competition Law and Economics*: 403-426.

years after *United Brands* the CJEU officially opened the door to "other methods" to estimate when the price charged by the dominant undertaking is unfair. Thus, the number of cases in this area has potentially increased. For instance, in the on-going investigations in the *Aspen* case, the EU Commission challenges for the first time the unfair prices charged by Aspen in relation to five cancer medicines patented by Aspen.[42] In the Statement of Objections, the EU Commission challenged Aspen's market behaviour, which increased the price of drugs only in some Member States by threatening to withdraw the product from the market. Finally, by accepting the comparison between different Member States, the Court established a link between the abuses concerning excessive and discriminatory pricing. As discussed in the following section, a dominant company that charges different prices in different EU Member States without objective justification breaches Art. 102(c) TFEU.

2.2. Discriminatory pricing: the long journey from *United Brands* to *MEO*

A dominant firm breaches Art. 102(c) TFEU when it applies "…dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage." Price discrimination falls within the scope of "dissimilar conditions". The discrimination can take different forms: besides the classical discrimination in the form of different retail/wholesale prices, the dominant company can discriminate its customers via selective price cuts and target rebates. Art. 102(c) TFEU clarifies that price discrimination is not abusive *per se:* a dominant company breaches this provision if it differentiates the price of its products/services in relation to "equivalent transactions", and by placing certain customers at a "competitive disadvantage" in comparison to "other trading partners". Finally, as further discussed in the following paragraphs, the CJEU case law has recognized that the dominant company can put forward "objective justifications" to justify its conduct.

The concept of "equivalent transactions" was first interpreted by the CJEU in *United Brands.* United Brands argued that the price of bananas differed among EU Member States "…due to fluctuating market forces, such as the weather, different availability of seasonal competing fruit, holidays, strikes, Government measures, currency denominations".[43] The Court, however, rejected these arguments: the

[42] EU Commission press release, "Antitrust: Commission opens formal investigation into Aspen Pharma's pricing practices for cancer medicines" (Brussels, 15.5.2017). The document is available at:
http://europa.eu/rapid/press-release_IP-17-1323_en.htm (22.5.2018).
[43] *Supra*, Case 27/6, para. 220.

CJEU noted that United Brands imported bananas of "similar quality" from Central/Latin America to Europe "in the same ships", "unloaded at the same cost in Rotterdam or Bremerhaven", and sold bananas "under the same 'Chiquita' Brand name under the same conditions of sale".[44] Therefore, since United Brands faced similar costs in order to supply the same type of product to its customers, the price disparity was in breach of Art. 102(c) TFEU. According to the Court, to determine if transactions involving the same product were indeed "equivalent", the EU Commission should analyse the "differences in transport costs, taxation, customs duties, the wages of the labour force, the conditions of marketing, the differences in the parity of currencies, the density of competition…."[45]. On the other hand, the Court pointed out that the different levels of demand of bananas in different EU Member States could not be sufficient to justify a persistent prices disparity within the EU common market.[46] *United Brands* case law has been constantly upheld in the following CJEU jurisprudence: the Court has generally looked at the nature of the product/service sold by the dominant company to its customers and assessed if the different supply costs faced by the dominant company made the transactions "equivalent".[47]

The concept of "competitive disadvantage" has also been interpreted by CJEU case law. Traditionally, the Court has "presumed" that price discrimination places the customer who pays the higher price for the same product/service in a competitive disadvantage in comparison to the "other trading partners" (i.e. its competitors). In particular, in *British Airways* the Court of Justice ruled that the EU Commission was not required to prove that the price discrimination caused "an actual quantifiable deterioration in the competitive position" of the discriminated customer.[48] Similarly, in *Clearstream* the General Court concluded the dominant company had placed some of its customers at a competitive disadvantage by charging higher prices for equivalent services over a period of five years; on the other hand, the General Court did not assess whether the price discrimination had resulted in a loss of market share for the discriminated customers.[49] In line with the traditional CJEU case law

[44] *Supra*, Case 27/6, para. 225.
[45] *Supra*, Case 27/6, para. 228.
[46] *Supra*, Case 27/6, para. 229.
[47] For instance, in *British Airways* the CJEU concluded that the sale of airlines tickets by British Airways (BA) to different travel agents in UK represented equivalent transactions. Although the tickets concerned different destinations, the CJEU considered equivalent the type of service provided by BA to the travel agents. Case C-95/04 P, *British Airways v. European Commission* (2007) ECLI:EU:C:2007:166, para. 136-141.
[48] *Ibid.*, para. 145.
[49] Case T-301/04, *Clearstream Banking AG and Clearstream International SA v. European Commission* (2009) ECLI:EU:T:2009:317, para. 194.

on Art. 102 TFEU, the EU Commission did not have to prove the effect of price discrimination on the competitive dynamics in the market.

The case law on "competitive disadvantage" has been revised by the CJEU in the recent *MEO* ruling.[50] The case concerned an alleged abuse of dominance by GDA (i.e. the Portuguese collective society of copyright holders), which charged different tariffs to its customers for the use of copyright materials.[51] In particular, the Portuguese television station MEO submitted a complaint to the Portuguese NCA, arguing to have paid higher tariffs to GDA in comparison to its competitors during the period 2010-2013.[52] The Portuguese NCA rejected MEO's claim due to the lack of evidence concerning the existence of a competitive disadvantage caused by the price discrimination.[53] On appeal, the Portuguese Competition Tribunal referred a preliminary ruling request to the CJEU, asking for a clarification of the concept of competitive disadvantage.[54] Similarly to *British Airways*, the Court ruled that Art. 102(c) TFEU does not require the EU Commission/NCA to "quantify" the competitive disadvantage suffered by the discriminated customer.[55] On the other hand, in line with the more effect-based approach to Art. 102 TFEU followed by the CJEU in the recent *Intel* ruling, [56] the Court also

[50] Case C-525/16, *MEO – Serviços de Comunicações e Multimédia SA v. Autoridade da Concorrência* (2018) ECLI:EU:C:2018:270.
[51] *Ibid.*, para. 5.
[52] *Ibid.*, para. 8.
[53] *Ibid.*, para. 12.
[54] *Ibid.*, para. 21.
[55] *Ibid.*, para. 27.
[56] The case concerned the compatibility of fidelity rebates granted by Intel to computer manufacturers with Art. 102 TFEU. In its previous case law, the Court had considered fidelity rebates as *per se* abusive, since they aimed at excluding the competitors of the dominant company. By contrast, in *Intel* the Court ruled that "not every exclusionary practice is necessarily detrimental to competition" (para. 134). In the judgment, the CJEU ruled that the EU Commission should consider a number of "relevant circumstances" to assess the effect of an abusive practice on competitive dynamics within the relevant market (e.g. share of the market affected by the anti-competitive conduct; duration of the conduct; exclusionary strategy by the dominant company), rather than considering a market conduct as abusive *per se* (para. 139). Finally, in *Intel* the CJEU recognized for the first time that Art. 102 TFEU sanctions only exclusionary practices that harm competitors "as efficient as" the dominant firm; Art. 102 TFEU cannot be relied on to protect inefficient firms.
The ruling concerned fidelity rebates, but the general wording of the ruling and the fact that the Court ruled the case as Grand Chamber suggest a shift in the Court case law towards a more effect-based approach in Art. 102 TFEU.

Case C-413/14 P, *Intel Corp. V. European Commission* (2017) ECLI:EU:C:2017:632.

For a comment of the *Intel* ruling see, Petit N., "The Judgment of the EU Court of Justice in Intel and the Rule of Reason in Abuse of Dominance Cases", forthcoming

added that the competition enforcer should take into consideration "…all the relevant circumstances" to determine whether price discrimination could produce a competitive disadvantage.[57] In particular, by analogy to *Intel*, the CJEU ruled that the NCA should take the following elements into consideration as relevant circumstances:[58]

> - the negotiation power of the customer of the dominant firm as regards the tariffs;
>
> - the conditions for charging those tariffs;
>
> - the duration and amount of the tariffs;
>
> - the existence of a strategy by the dominant firm aiming to exclude from the downstream market one of the trading partners "which is at least as efficient as its competitors".

In the specific case, the Court noted that MEO had a strong buyer power, and its market share had not decreased during the period of the alleged price discrimination.[59] Secondly, the contested tariffs had been determined by a previous arbitral award, rather than by the independent GDA decision.[60] Taking into consideration these two "relevant circumstances", the Court concluded that the discriminatory tariff had not placed MEO in a "competitive disadvantage", and thus it did not breach Art. 102 TFEU.[61]

In *MEO*, the CJEU extended the more effect-based analysis of Art. 102 TFEU to exploitative abuses. In particular, the references to the assessment of the "relevant circumstances" and to the "as efficient competitor" clearly come from the recent *Intel* ruling. On the one hand, *MEO* should be welcome, since it aligns the CJEU case law in relation to the analysis of different categories of abuses under Art. 102 TFEU. On the other hand, *MEO* has also increased the burden of proof that the EU Commission/NCA faces to prove the existence of discriminatory pricing under Art. 102(c) TFEU: although the competition enforcer does not have to quantify the competitive disadvantage, it has to show that the price disparity is capable of having a negative effect on the discriminated customer (e.g. lower market share).

---

in the *European Competition Journal*, October 2018. The paper is available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3086402 (22.5.2018).

[57] *Supra*, Case C-525/16, para. 28.

[58] *Supra*, Case C-525/16, para. 31.

[59] *Supra*, Case C-525/16, para. 32.

[60] *Supra*, Case C-525/16, para. 33.

[61] *Supra*, Case C-525/16, para. 34.

While the EU Commission/NCA faces the burden of proof concerning the existence of equivalent transactions and the competitive disadvantage suffered by the discriminated customers, the dominant firm can put forward "objective justifications" to show the legality of the price disparity.[62] For instance, the dominant firm could argue that the price disparity is caused by demand fluctuations. As mentioned above, in accordance with *United Brands* case law such an argument would not be accepted by the Court to show the lack of "equivalence" among different transactions,[63] while it could be put forward by the dominant company as a possible justification. While objective justifications are possible in theory, in practice they have been rarely accepted by the Court. This is due to the fact that most of the cases sanctioned under Art. 102(c) TFEU concern forms of price discrimination connected to the customers' nationality; i.e. cases that have a close link with the EU internal market integration. For instance, in *Corsica Ferriers* the Court sanctioned Genoa seaport authority for charging higher tariffs for its piloting services to Corsica Ferriers (i.e. a French flagship company) in comparison to the other Italian vessels.[64] Similarly, in *Irish Sugar* the General Court sanctioned the dominant manufacturer of raw sugar in Ireland, since it granted rebates only to the wholesalers that distributed sugar in Ireland, and not to the customers that exported sugar to other EU Member States.[65] In *United Brands,* the CJEU emphasized that the price discrimination among customers based in different Member States represented a *per se* abuse; in its ruling, the Court did not analyse any objective justification that explained the price disparity.[66] However, taking into consideration the more effect-based approach to price discrimination followed by the Court in *MEO,* it remains unclear whether and to what extent the Court will continue to exclude in the future the possibility to put forward objective justifications *vis-à-vis* forms of price discrimination linked to internal market considerations.

Discriminatory pricing can have either an exclusionary dimension (e.g. via a margin squeeze strategy, a vertically integrated company sells a product/service at a higher price to a downstream competitor in comparison to its subsidiary) or an exploitative one (i.e. the dominant company sells the same product at different prices/conditions to its customers/consumers). By referring to the

[62] *Supra,* Case T-301/04, para. 185.
[63] *Supra,* Case 27/6, para. 229.
[64] Case C-18/93, *Corsica Ferries Italia Srl v. Corpo dei Piloti del Porto di Genova* (1994) ECLI:EU:C:1994:195.
[65] Case T-228/97, *Irish Sugar v. European Commission* (1999) ECLI:EU:T:1999:246, para. 125.
[66] "A rigid partitioning of national markets was thus created at price levels, which were artificially different, placing certain distributor/ripeners at a competitive disadvantage, since compared with what it should have been competition had thereby been distorted."
Supra, Case 27/6, para. 233.

expression "other trading partners", Art. 102(c) TFEU adopts a broad language, which refers to both categories of abuses. However, due to the risk of price regulation and overlaps with sector regulation, Art. 102(c) TFEU has traditionally been relied on by the EU Commission and NCAs to sanction only exclusionary abuses.[67] The recent *MEO* ruling is likely to further strengthen this enforcement tendency. In his opinion in *MEO*, Advocate General (AG) Wahl argued that while a vertically integrated company has an incentive to discriminate some of its customers to the benefit of its own subsidiary, exploitative forms of price discrimination are "extremely rare".[68] According to the AG, a non-vertically integrated firm does not have any incentive to discriminate some of its customers, since this strategy would negatively affect its reputation and it would not create any benefit for the dominant firm in terms of market share.[69] In its ruling in *MEO*, the Court followed the AG's sceptical view *vis-à-vis* exploitative price discrimination.[70] By introducing a presumption that exploitative price discrimination is unlikely to take place in the market and by increasing the burden of proof faced by the EU Commission/NCA to show the existence of a competitive disadvantage, the Court has reduced the scope of application of Art. 102(c) TFEU *vis-à-vis* exploitative price discrimination. As further discussed in Section 4.2, this enforcement choice is debatable in the context of the data economy: by relying on algorithms and "big data", dominant online platforms can introduce quasi-individual pricing for their customers. This conduct might indeed be covered by Art. 102(c) TFEU as an exploitative form of price discrimination.

2.3. Contractual clauses and abuse of dominance

In its jurisprudence, the CJEU has sanctioned under Art. 102 TFEU a large number of contractual clauses imposed by the dominant company on its customers. For instance, in *United Brands* the CJEU considered unfair the fact that the distributors of United Brands could

[67] *United Brands* is one of the rare cases where the EU Commission was successful in challenging an exploitative discriminatory pricing under Art. 102 TFEU*:* while the EU Commission was not successful in challenging the excessive prices of Chiquita bananas, the EU Court of Justice recognized as abusive the fact that the price of bananas differed from country to country within the EU common market.

[68] Opinion of Advocate General Wahl delivered on 20th December 2017 in the Case C-525/16, *MEO – Serviços de Comunicações e Multimédia SA v. Autoridade da Concorrência*, ECLI:EU:C:2017:1020, para. 80

[69] *Ibid.*, para. 79.

[70] "… in a situation such as that at issue in the main proceedings where the application of differentiated tariffs concern only the downstream market, the undertaking in a dominant position, in principle, has no interest in excluding one of its trading partners from the downstream market…"
Supra, Case C-525/16, para. 35.

not sell un-ripened bananas.[71] Similarly, in *Porto di Genova* the Court considered unfair the fact that the maritime companies were obliged to rely on the docking services provided by the firm appointed by Genoa seaport authority, rather than being able to freely choose the service provider.[72] Finally, in *GVL* the Court ruled that the German copyright collective society breached Art. 102 TFEU when it imposed contractual conditions that were less favourable to foreign artists than to the German ones.[73] The Court has never provided either a complete list of contractual clauses considered unfair or a general definition to this regard. However, by analysing its case law, we could deduct some general criteria.

First of all, in the cases mentioned above the CJEU has generally sanctioned contractual clauses imposed by the dominant company on industrial customers, rather than final consumers. Therefore, the Court has never discussed the overlap between competition and consumer protection law in this line of cases. However, as further argued in the following section, in our view this does not prevent in principle the application of Art. 102 TFEU to sanction unfair contractual clauses imposed by a dominant company that directly harm final consumers.

Secondly, the Court has considered contractual clauses in breach of Art. 102 TFEU when they have been "unilaterally" imposed by the dominant company; in other words, when the dominant company is an unavoidable trading partner for the customer. As discussed in the previous section in relation to *Corsica Ferriers*, the dominant company could be either *de facto* (e.g. *United Brands)* or *de jure* (*e.g. Porto di Genova, GVL)* an unavoidable trading partner for the customer. In such a scenario, the dominant company could leverage its dominant position in negotiating the contractual clauses.

Thirdly, there are different ways whereby contract clauses could be considered unfair. For instance, the dominant company obliges its customers to purchase services either not requested or not closely related to the core subject of the contract. For instance, in *Alcatel* the CJEU considered unfair the contractual clause whereby a rent contract concluded between the dominant company and another firm would be automatically extended after its expiration, and the firm would be automatically required to pay a higher rent to the dominant firm.[74] Similarly, in *BRT* the CJEU considered abusive the clause whereby artists were required to transfer the management of their copyright

[71] *Supra,* Case 27/6, para. 130-162.
[72] Case C-179/90, *Merci convenzionali porto di Genova SpA v. Siderurgica Gabrielli SpA.* (1991) ECLI:EU:C:1991:464, para. 3.
[73] Case 7/82, *Gesellschaft zur Verwertung von Leistungsschutzrechten mbH (GVL) v Commission of the European Communities* (1983) ECLI:EU:C:1983:52, para. 47.
[74] Case C-247/86, *Société alsacienne et lorraine de télécommunications et d'électronique (Alsatel) v. SA Novasam.*(1988) ECLI:EU:C:1988:469.

works to SABAM (i.e. Belgian collective society of copyright owners) even after the end of the contract.[75] In particular, the Court ruled that SABAM breached Art. 102 TFEU by "…. imposing on its members obligations which are not absolutely necessary for the attainment of its object and which thus encroach unfairly upon a member's freedom to exercise his copyright".[76] Furthermore, in line with the internal market considerations discussed in the previous section, contractual discrimination of customers based in different Member States has consistently been considered abusive (i.e. *GVL).* Finally, contractual clauses have been considered abusive when the dominant company imposes them to facilitate other types of abuses. For instance, United Brands prohibited its distributors to sell green bananas, in order to keep a control over the price of bananas sold in different Member States and thus to differentiate the price of bananas in different countries.

Finally, in its jurisprudence on unfair contractual clauses the Court analysed possible objective justifications put forward by the dominant company. For instance, in *AAMS* the Italian monopoly in charge of the distribution of cigarettes in the country tried to justify the contractual clauses limiting the ability of foreign suppliers to sell cigarettes in Italy.[77] In particular, AAMS argued that these clauses were necessary in view of the limited capacity of its distribution network.[78] The EU General Court did not ultimately accept these justifications, ruling that "AAMS had not proved to the requisite legal standard that the clauses mentioned above were necessary to protect its commercial interests and to avoid the risk of its distribution network becoming overloaded…."[79] However, it is worth noting that the General Court was open to analyse the arguments put forward by the dominant firm. Therefore, from a comparative perspective, the Court seems to accept that a dominant company may put forward justifications for all types of exploitative conducts analysed in section 2. The only exception is price discrimination among customers based in different EU Member States: due to internal market considerations, the Court has in fact followed a quasi *per se* approach in this regard.

[75] Case 127/73, *Belgische Radio en Televisie and société belge des auteurs, compositeurs et éditeurs v SV SABAM and NV Fonior* (1974) ECLI:EU:C:1974:25.
[76] *Ibid.*, para. 15.
[77] Case T-139/98, *Amministrazione Autonoma dei Monopoli di Stato (AAMS) v. European Commission* (2001) ECLI:EU:T:2001:272.
[78] *Ibid.*, para. 56-64.
[79] *Ibid.*, para. 79.

3. The scope of application of EU competition law in the data economy

After this analysis of the traditional CJEU case law in relation to different types of exploitative abuses, we will discuss the scope of application of EU competition law in the context of the data economy in this section. In our journey towards the *terra incognita,* we leave the well-known seas of the CJEU case law and (in section 3.1) discuss possible market failures in the data economy that justify EU competition law intervention. In particular, we discuss the limits of data protection law in the context of the data economy by looking at the "privacy paradox" and its corresponding implications. For instance, we analyse what role the (very common) lack of transparency of data protection terms plays. Aside from the "privacy paradox", we will look at the role of anonymization of personal data by online platforms, and the problems that might come up when anonymization is not effective. These issues are considered potential "market failures"; i.e. situations that might justify an intervention by EU competition law. Section 3.1, therefore, discusses "why" EU competition law should have a role to play in the data economy, leaving the discussion of specific issues related to exploitative abuses to section 4.

By contrast, section 3.2 analyses the arguments usually put forward in the literature against EU competition law intervention *vis-à-vis* exploitative abuses. On the one hand, section 3.2.1 analyses the economists' arguments against the enforcement of Art. 102 TFEU to sanction excessive and discriminatory pricing. In particular, section 3.2.1 discusses the "filters" that a number of economists have developed to limit the scope of EU competition law intervention in this area in light of the relevant CJEU case law. On the other hand, section 3.2.2 analyses the objectives, scopes of application and enforcement structures of competition, data protection and consumer law. Due to overlaps among these three policy areas, some authors have argued that EU competition law should leave the task of sanctioning unfair contractual clauses in the context of the data economy to data protection and consumer law. Section 3.2.2 challenges this argument: in spite of their "family ties", these three policies have different objectives, scopes of application and enforcement structures, and thus they cannot replace each other.

To sum up, section 3 provides a preliminary discussion on the scope of application of EU competition law in the context of the data economy. This discussion is necessary to "map" the *terra incognita.*

3.1. Market failures in the data economy

3.1.1. The economics of privacy: when do markets fail in the data economy?

In this section, we analyse market failures in the data economy which are (at least in part) caused by exploitative abuses of dominance. The focus here lies on those business models that trigger the applicability of data protection law and as such have implications for privacy matters. The newly enacted General Data Protection Regulation is applicable (only) when personal data are processed: Art. 2(1) GDPR.[80] As soon as this is the case, data controllers are responsible to ensure compliance with the provisions given under the GDPR and the rights afforded to the data subjects.[81] In order to further define our scope of analysis, we need to take a quick look at the characteristics of the economics of privacy. In the course of this text, we use the traditional definition of privacy as being "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others."[82]

Economic analyses of privacy have shown that it is not possible to give a clear, uniform answer to the question whether or not the disclosure of personal data is beneficial for data subjects (here: final consumers, users) or data controllers (here: market dominant companies, undertakings) respectively.[83] Generally speaking, economic efficiency in privacy matters depends on many diverse factors, such as the respective market, the individual preferences of

[80] The GDPR defines personal data as "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" (Art. 4(1) GDPR).

[81] The GDPR defines controllers as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its
nomination may be provided for by Union or Member State law" (Art. 4(7) GDPR). A data subject is, according to Art. 4(1) GDPR, an "identified or identifiable natural person (…); 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".

[82] Westin A. F., *Privacy and Freedom* (1970), p. 7. On the definition of privacy more generally, see Solove, D. J. (2005), 'A Taxonomy of Privacy' 154(3) *University of Pennsylvania Law Review:* 477, p. 486–487.

[83] Kerber W. (2016), "Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection" 65(7) *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil:* 639, p. 640.

those concerned, and the specific situation. As a rule of thumb, data controllers benefit from an increasing disclosure of personal data on the user side, which is why they tend to collect as many user data as possible.[84] Yet, this beneficial effect does not necessarily have to be the case all the time.[85] Furthermore, in many situations data subjects benefit from data disclosure, too, since they can enjoy personalized and better services. Nevertheless, economic research shows that these effects are context-sensitive, and therefore no general statements can be made.

3.1.2. The economics of privacy: an adjusted definition of "market failure"

One specific feature of the data economy and one of the reasons for these "blurred" and ambiguous results is that the economic value of privacy is twofold in nature.[86] Privacy can serve, firstly, as an intermediate good, which is the case in those situations when the non-disclosure of information is beneficial for the data holder.[87] This might be the case, for instance, if an individual does not want an insurance company to know about certain personal information (e.g. concerning hereditary diseases running in one's family); information that might give the insurer reason not to enter into an insurance contract with the person concerned at all, or under unfavourable conditions only.[88] Correspondingly, privacy rights might be economically beneficial in those cases where individuals can deliberately chose to disclose personal data *in lieu* of a monetary payment, in order to access certain services, such as smartphone apps or web-based services.[89] Apart from this first dimension, which in theory allows the assignment of a certain monetary value to privacy rights, privacy serves as a "final good".[90] This dimension of privacy is based entirely on personal preferences and has a normative origin and character. Its legal protection finds its origin in constitutional documents, most notably Art. 8 of the EU Charter of Fundamental Rights ("Protection of personal data") and Art. 8 of the European Convention on Human Rights ("Right to respect for private and family

[84] Cf. Acquisti A. (2010), "The Economics of Personal Data and the Economics of Privacy: Joint WPISP - WPIE Roundtable: The Economics of Personal Data and Privacy - 30 Years after the OECD Privacy Guidelines", p. 8-9.
The text is available at https://www.oecd.org/sti/ieconomy/46968784.pdf (22.5.2018).
[85] *Ibid.*, p. 12-14.
[86] Farrell J. (2012), "Can Privacy Be Just Another Good?" 10 *Journal on Telecommunications and High Technology Law:* 251, p. 252.
[87] *Supra,* Kerber (2016), p. 640.
[88] Cf. *supra,* Farrell (2012), p. 252.
[89] *Supra,* Kerber (2016), p. 640.
[90] *Ibid.*

life").[91] Most people feel a need for at least a certain degree of privacy *per se*, independent of financial considerations. Privacy preferences are personal and diverse by nature.[92] What one person considers being highly sensitive information about him or her might be easily and willingly disclosed by someone else. Taking this unique character of privacy into consideration, one of the functions of data protection law is to find a balance between the different interests at stake, since different parties benefit – depending on the situation – from the disclosure or non-disclosure of personal data in economic terms. Therefore, as an additional normative layer on top of this economic dimension, privacy deserves protection *per se*.[93]

These factors explain why we chose to approach the question whether or not there is a market failure by using a broader, somewhat unorthodox approach to this term. Our definition does not look primarily at Pareto efficiency, as is usually the case when market failures are analysed. We rather borrow from Alessandro Acquisti by asking: "will market forces be able to maintain a desirable balance between privacy and disclosure, in a world where most of our personal and professional lives unfold trails of electronic data, and where powerful economic interests favor information availability over information protection?"[94]

In assessing this question, it is necessary to look at both the data subjects' and the data controllers' side and how they interact with each other. In our analysis, it is assumed that the data controllers are market dominant firms. We start by looking at the role of consent under the GDPR, since this legal framework significantly predetermines and shapes the behaviour of the abovementioned market players.

3.1.3. The regulation and notion of consent under the GDPR

The GDPR relies on the traditional principle under EU data protection law that the processing of personal data is prohibited, unless a legal

[91] The European Court of Human Rights has acknowledged in its case law that the right to privacy as given in Art. 8 of the European Convention on Human Rights must be interpreted to include a right to data protection, cf. *Leander v. Sweden*, judgment of 26 March 1987 (Application no. 9248/81) and *Rotaru V. Romania*, judgment of 4 May 2000, (Application no. 28341/95).
[92] *Supra*, Farrell (2012), p. 251-252.
[93] For an extensive overview of the benefits and costs of disclosing personal data, cf. *supra*, Acquisti (2010), p. 7-19.
[94] Acquisti A. (2012), "Privacy and Market Failures: Three Reasons for Concern, and Three Reasons for Hope" 10 *Journal on Telecommunications and High Technology Law:* 227, p. 227.

basis for the processing can be invoked by the data controller.[95] Art. 6(1) GDPR provides an exhaustive list of legal bases, such as contractual necessity[96] and legitimate interests pursued by the data controller[97]. One prominent and widely relied legal basis is consent given by the data subject: Art. 6(1)(a) GDPR.[98] Art. 4(11) GDPR states that consent "means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". Article 7 GDPR further specifies the conditions for valid consent. For instance, the burden of proof that consent was given in the first place lies with the data controller (Art. 7(1) GDPR), and the data subject is free to withdraw consent at any time (Art. 7(3) GDPR). In the Recitals of the GDPR, further and more detailed explanations are given.[99] When it comes to the processing of special categories of personal data, such as those revealing the racial or ethnic origin of the data subject or those concerning their health, Art. 9 GDPR is applicable. The processing is prohibited in these cases, unless one of the exceptions as given in Art. 9(2) GDPR applies, such as when the data subject has given "explicit consent" to the processing (i.e. Art. 9(2)(1) GDPR). The term "explicit consent" – as opposed to "consent" – has not been defined in the GDPR, even though it is used several times within the Regulation.[100] In these cases, an express statement of consent is necessary, thereby raising the threshold when it comes to *how* consent is given by the data subject.[101]

The idea that consent serves as a legal basis for the processing of personal data mirrors the notion of "informational self-determination"[102] – i.e. one of the leading principles of European data

[95] This was also the case under the Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995, p. 31-50, hereinafter referred to as "DPD"), cf. Art. 7 DPD. The role of consent has not changed significantly with the enactment of the GDPR (apart from the extension of its definition that consent now also has to be *"unambiguous"*, Art. 4(11) GDPR. This requirement was not included in the DPD's definition of consent, cf. Art. 2(h) DPD).

[96] Art. 6(1)(b) GDPR.

[97] Art. 6(1)(f) GDPR.

[98] We exclude from our analysis the situation that consent is given by a child, cf. Art. 8 GDPR.

[99] See in particular Recitals 32, 33, 42 and 43 GDPR.

[100] Cf. Art. 22(2)(c), 49(1)(a) GDPR.

[101] Express consent does not necessarily have to be given in writing, but the express character of its granting must be ensured (Article 29 Data Protection Working Party (2017), "Guidelines on Consent under Regulation 2016/679: 17/EN WP259", p. 18–19, available at http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=50053 (22.5.2018)).

[102] This term was created by the German Federal Constitutional Court in its judgment on a national census in 1983 ("*Volkszählungsurteil*") and was expressly acknowledged by the Court as a fundamental right (*"Recht auf informationelle*

protection law. The rule that consent gives a legal basis for the processing of personal data aims at allowing data subjects to decide autonomously whether and to what extent personal data relating to them can be processed.[103] In the context of consent, Art. 4(11) GDPR names four requirements that must be complied with: consent must be freely given, specific, informed, and unambiguous.[104] When looking at these requirements under Art. 6(1)(a) and 7 GDPR and the corresponding Recitals, it becomes clear that the GDPR follows the idea that data subjects should have full knowledge and control over what is happening with "their" personal data when granting consent. Data subjects are deemed to act autonomously and fully informed of all facts necessary to evaluate what is happening to their data: who has access to the data, how they are processed, and what the corresponding future implications might be. Both the willingness and the actual ability to decide autonomously whom to give consent form the basis for the function of consent under the GDPR, as expressed by the terms "freely given" and "informed". Thus, the approach taken by the GDPR is in line with traditional privacy literature which assumes that adequate privacy protection will be achieved by giving data subjects control over their personal data.[105]

In practice, this idealized picture of effective informational self-determination and autonomy in many situations does not live up to its goals. The user side oftentimes does not act as envisaged by the drafters of the GDPR. Data holders know this and in many situations act accordingly, in order to collect as many data about the users of their services as possible and to maximize their profit.

3.1.4. The "privacy paradox"

To better understand why markets may fail in the data economy, it is necessary to take a closer look at the so called "privacy paradox". This expression refers to the phenomenon that a broad majority of users claim to care about their privacy and the need for data protection,

Selbstbestimmung"), Bundesverfassungsgericht, judgment of 15 December 1983, NJW 1984, p. 419.

[103] Buchner B., Petri T. in Kühling J. and Buchner B. (eds), *Datenschutz-Grundverordnung: Kommentar* (2017), Art. 6, para. 17.

[104] When analysing the regulation under the GDPR, one finds that most sections and Recitals dealing with consent serve to specify one of these requirements (or provide requirements of a formal nature, such as Art. 7(2) GDPR). For instance, the requirement that consent be "freely given" is specified further in Art. 7(4) GDPR, "specific" corresponds to Art. 5(1)(b) and 6(1)(a) GDPR and "unambiguous" corresponds to Recital 32, see Buchner B., Kühling J. in Kühling J. and Buchner B. (eds), *Datenschutz-Grundverordnung: Kommentar* (2017), Art. 4 Nr 11, para. 6-10.

[105] Cf. Brandimarte L., Acquisti A., Loewenstein G. (2012), "Misplaced Confidences: Privacy and the Control Paradox" 4(3) *Social Psychological and Personality Science*: 340, p. 341.

while in reality they do not act according to these expressed preferences and desires.[106] Internet users oftentimes disclose personal data freely, and give consent to the processing of their personal data by simply "agreeing" with online "terms and conditions" and privacy policies without properly reading, let alone understanding them.[107] According to Kerber, studies on this subject have revealed a couple of general findings.[108] Firstly, users' behaviour in this area is highly context-specific. As such, what kinds of information data subjects disclose depends on the particular circumstances. Secondly, privacy preferences of internet users are heterogeneous. This means that their willingness to disclose information varies significantly, and is also dependent on the respective recipient. Thirdly, it has been proven that many users lack awareness of the extent of both the data collection and the corresponding high level of behavioural targeting users face accordingly. Fourthly, bounded rationality and behavioural decision-making biases also play a role in this context.

What does all of this have to do with privacy, data protection and the function of consent under the GDPR? The privacy paradox can be linked to two problems that can subsequently lead to market failures, which in turn are related to a "consent dilemma". Firstly, on the one hand users do care about data protection, but on the other hand they are not willing to act accordingly and take measures to actually protect them – i.e. such as carefully reading privacy policies or using privacy enhancing technologies on their computers. Users know that it might be reasonable to be more careful and deliberate, but out of a mixture of "wilful data negligence" and laziness they do not act upon their own standards. Secondly, due to a lack of transparency of data-related processes and intelligibility of declarations of consent, users do not know what happens to their data. The "root" of this problem is not unwillingness or laziness on the user side, but rather a lack of ability: Even if users put effort into making an informed choice, this is not (or barely) possible for them. Oftentimes, the two problems mix: most privacy policies on websites are so long that barely any user would be willing or able to take the time to read them. At the same time, the language used is barely comprehensible to lay people.

[106] *Supra,* Kerber (2016), p. 641-642.
[107] German Monopolies Commission (2015), "Competition policy: The challenge of digital markets (Special Report No 68): Special Report by the Monopolies Commission pursuant to section 44(1)(4) of the Act Against Restraints on Competition", p. 74, para. 309.
The text is available at
www.monopolkommission.de/images/PDF/SG/s68_fulltext_eng.pdf (22.5.2018).
[108] *Supra,* Kerber (2016), p. 642.

3.1.5. Markets do not cater for users' privacy preferences

Looking at this dilemma from an economics perspective, the following situation emerges. Internet users declare clear preferences for a specific amount of privacy protection when using certain web services, such as search machines and social networks. Yet, the market usually does not provide as many privacy options as would be necessary to cater for these preferences.[109] For instance, when it comes to social networks, direct network effects can ultimately lead to market concentration.[110] This, in turn, can lead to the situation that new and existing users are faced with a "take it or leave it" lockup, and have to either consent to the terms given, or abstain from using the service at all.[111] A well-functioning competitive market would be able to satisfy these demands and offer different options that fulfil different privacy preferences. For example, it would be feasible that a social network offers the option to restrict its collecting and processing of personal data to the minimum necessary and refrains from using the data for marketing purposes in exchange for a monthly payment.[112] This would allow those users who value their privacy higher than the monthly payment to satisfy these preferences. Yet, in the digital economy business models oftentimes offer their services for "free", in the sense that they do not demand a monetary payment. On the other hand, these websites monetize the users' data, since those data can be used for targeted advertising, market analytics, and many more profitable causes.[113] Privacy-friendly options are often not offered, and the users are not adamant enough to demand them. Therefore, only few market players see a necessity to satisfy the demand given. In general, companies rarely compete based on the privacy quality of their services.[114]

As we have seen, the background to this unsatisfactory situation is twofold: direct network effects (and other reasons) lead to market concentration and dominance, so that users have no or only a limited choice which service to use. At the same time, their behaviour is irrational insofar that their high demand for privacy and data protection does not make them act accordingly on the market, as most people tend to still use the "free" services. Eventually, these factors make users agree to privacy policies, because they neither have a real

[109] *Ibid.*
[110] *Supra*, German Monopolies Commission (2015), p. 75, para. 311.
[111] *Ibid.*; Custers B. et al. (2013), "Informed Consent in Social Media Use - The Gap between User Expectations and EU Personal Data Protection law" 10(4) *SCRIPTed:* 435, p. 456-457.
[112] *Supra*, Kerber (2016), p. 642.
[113] Cf. s*upra*, German Monopolies Commission (2015), p. 20, para. 40.
[114] Cf. *Autorité de la Concurrence* and *Bundeskartellamt* (2016), "Competition Law and Data: Joint paper", p. 24-25. The text is available at: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2 (22.5.2018).

choice nor they really act according to their preferences. In situations like these, consent oftentimes cannot be seen as meeting the conditions given in Art. 4(11) GDPR. In particular, it can be highly doubted whether consent under these circumstances is "freely given" and "informed" – i.e. its granting turns out to be not more than mere fiction and an act of formalism, aimed at ensuring legal compliance.[115] As such, a market failure within the meaning of the abovementioned definition is given, since the balance between privacy and data disclosure in these situations runs counter to the clear preferences of the users (and to the intention the lawmaker had when drafting the GDPR), and the markets are not able to satisfy the (privacy) demands users have.

3.1.6. Lack of transparency as a market failure

A second market failure can be seen in the lack of transparency users face when giving consent online.[116] Oftentimes, users do not know to what extent their personal data are collected, processed and passed on to third parties. As a result of information asymmetry, they are not always able to make well-informed rational decisions.[117] This market failure can also be traced back to the problematic role of consent, but it is different in nature. Above, we have described that markets fail to deliver solutions to the privacy preferences users have. Here, the problem is that internet users regularly consent to the collection and processing of their personal data, even though they are not (or barely) able to foresee what is happening to them. Not being able to make a choice in an informed manner, even if one wanted to, is the main problem here.

Again, privacy policies used by online services are part of the problem. It has been found that internet users do not actually read them, but often rather blindly accept them.[118] For example, for a 2015 survey requested by the European Commission, 21.707 people were asked to what extent they read privacy policies on the internet. It was found that only 18 % of the respondents fully read them, while 31% do not read them at all, and 49% only read them partially.[119] Furthermore, these policies are often very long and drafted in a manner that most users do not understand, and usually drafted using a

[115] *Supra,* Buchner/Kühling in Kühling/Buchner (2017), Art. 7, para. 10.
[116] *Supra,* Kerber (2016), p. 642.
[117] *Ibid.*
[118] *Supra,* Custers et al. (2013), p. 457; *supra,* Autorité de la concurrence and Bundeskartellamt (2016), p. 25.
[119] European Commission, "Data Protection – Report: Special Eurobarometer 431" (Brussels 2015), p. 84 http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf (22.5.2018). The remaining 2 % answered *"Don't know"*.

wide formulation that is open to interpretation.[120] Already in 2008, researchers found that if the average US-American internet user had to read all privacy policies he or she typically encounters during the course of a year, this endeavour would take him or her about 201 hours of reading time in total.[121] Thus, users "agree" with policies at large, but are not aware what exactly they consent to.

Looking at this issue from yet another angle, another layer of potentially significant privacy implications has to be taken into consideration. Empirical research has found that giving users more (perceived) control over the release of personal information relating to them paradoxically leads to the effect that, as a result, they are willing to disclose more sensitive (and potentially harmful) information.[122] The study finds that "'more' control can sometimes lead to 'less' privacy in the sense of higher objective risks associated with the disclosure of personal information."[123] Thus, having users agree to privacy policies – typically by ticking a box – can make them feel safe and foster their disclosing even more personal data. Again, with a view to the GDPR's notion of consent, a "desirable balance between privacy and disclosure" is not given under these circumstances.

3.1.7. The problem of anonymization of personal data

The last market failure we analyse also has to do with privacy implications for users resulting from automated data processing. Yet, this problematic imbalance neither has to do with the privacy paradox nor with consent. Instead, it is of a rather technical nature outside of the influence of consumers.

Traditionally, the rules on data protection only apply if "personal data" are processed.[124] One decisive factor when distinguishing between personal and non-personal data is the identifiability of the person concerned – i.e. the possibility of singling the person out of a hypothetic group of people. The natural person the information pertains to must be identified or identifiable.[125] Recital 26

[120] *Supra*, Custers et al. (2013), p. 457
[121] McDonald A. M., Cranor L. F. (2008), "The Cost of Reading Privacy Policies" 4(3) *I/S: A Journal of Law and Policy for the Information Society:* 543, p. 565.
[122] *Supra*, Brandimarte/Acquisti/Loewenstein (2012), p. 345-346.
[123] *Ibid.*, p. 345.
[124] Cf. Art. 2(1) GDPR, Art. 3(1) DPD.
[125] 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*": Art. 4(1) GDPR.

GDPR helps to further carve out the definition and quality of personal data by stating that

"[t]o determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."

As we can see, the term "personal data" is relative in nature.[126] In many situations, determining whether or not data qualify as "personal" is fairly easy, in particular when identifiers such as name, address, and social security number are included in a dataset. Yet, in other situations this determination is more complicated, as it depends on the individual context and the means available to both the controller and third parties to find out who the data relates to. This goes hand in hand with the question of how likely it is that someone tries to find out the identity of the person "behind" the data. Thus, the very same set of data could be deemed personal or non-personal, depending on situation, context, data controller, and availability of further datasets that in combination allow for identifying the natural persons.[127] In some situations, it is hard to determine the "tipping point" when data qualify as personal.[128] Many questions in this regard remain unclear, also due to the rapid technological developments in recent years and the ever-increasing mass of data available.

Data protection law is not applicable once anonymous data are processed, i.e. "information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable" (Recital 26 GDPR). The GDPR indirectly provides for a further classification within anonymous data. This distinction does not have any direct legal significance, yet it helps in understanding and structuring. Anonymous data can be further distinguished between those which are not personal from the outset (such as weather data or machine data[129]) and those that had been personal but have been rendered anonymous through further processing, for instance by deleting identifiers. The latter kind of data are what we consider to be

[126] Gola P. in Gola P. (ed), Datenschutz-Grundverordnung: VO (EU) 2016/679 - Kommentar (2017), Art. 4, para. 17.
[127] Cf. *ibid.*, Art. 2, para. 10-11.
[128] Cf. *ibid.*
[129] Of course, this kind of data can easily turn personal, too, once it is combined with personal data.

the problematic ones here. Rendering data anonymous in an effective manner (i.e. one that securely prevents re-identification) is a cumbersome process.[130] Even though anonymization of data in many situations lowers their usefulness, it sometimes is a tempting route for data controllers to follow, as it frees them from the burdens that data protection compliance brings along.[131] Yet, it is also a critical step, since data that have been rendered "anonymous" in a manner that is not effective may be considered personal, and thus still trigger the applicability of data protection law. As regards legal certainty and in particular the administrative fines given under Art. 83(5) GDPR, the question of how to effectively anonymize data thus remains vital for data controllers.

Data controllers often wrongly assume that anonymization of personal data is effective. For instance, anonymous data can be sold freely without any restrictions stemming from data protection regulation. Yet, if the buyer is able to reverse the process, he or she may suddenly have access to masses of personal data. This is a situation the GDPR actually aims to avoid. Yet, the Regulation failed to provide a more nuanced approach to the concept of personal data, but rather chooses an "all or nothing" approach.[132] Re-identification oftentimes is easier than one might expect, and quite often surprisingly few information allow finding out the identity of those people who should, actually, not be identifiable anymore.[133] Especially when access to other datasets is given, this can serve as a key to the identities "hidden" in anonymized data. For instance, a study conducted by Latanya Sweeney in 2000 found that knowing gender, date of birth and 5-digit ZIP-code of a person might be enough to identify 87 % of the United States' population.[134] Today,

[130] For an illustrative example, see Ohm P. (2010), "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" 57(6) *UCLA Law Review:* 1701, p. 1711-1716.

[131] More generally on why companies (try to) anonymize data: *ibid.*, p. 1708-1710.

[132] On this issue more generally and from a US-American perspective see Schwartz P. M., Solove D. J. (2011), "The PII Problem: Privacy and a New Concept of Personally Identifiable Information" 86 *New York University Law Review:* 1814, who propose a new concept of personally identifiable information (a similar, yet not identical equivalent to personal data under EU law) that provides for a "*continuum of risk of identification*" in order to tackle the different privacy implications that come along with different kinds of data and situations as regards identifiability of natural persons.

[133] Cf. *supra*, Ohm (2010), p. 1717-1722 for several examples.

[134] Cf. Sweeney L., "Simple Demographics Often Identify People Uniquely" (Pittsburgh 2000), Carnegie Mellon University, Data Privacy Working Paper 3, p. 2, who also found that "*[a]bout half of the U.S. population (132 million of 248 million or 53%) are likely to be uniquely identified by only {place, gender, date of birth}, where place is basically the city, town, or municipality in which the person resides. And even at the county level, {county, gender, date of birth} are likely to uniquely identify 18% of the U.S. population. In general, few characteristics are needed to uniquely identify a person.*" It should be noted, though, that much more information

"internet of things" devices, such as fitness trackers or smart phones, are a serious risk for misled claims of effective anonymization.[135] The latter devices are widely spread and equipped with all kinds of sensors that allow tracking the location of the phone (and its owner, correspondingly), its velocity, temperature of the surroundings, and much more. Access to this data allows building highly detailed profiles of people and their daily lives and activities. The more detailed these profiles are, the harder it is to anonymize them effectively. For example, a few pieces of information that distinguish one person from others may suffice to disclose this person's whole profile when access to poorly anonymized datasets collected by the device is given.[136]

The problem we encounter here is outside of the realms of the privacy paradox: it has nothing to do with users' own actions and the consent dilemma described above. Once data are not considered to be personal anymore, the legal obligations stemming from the GDPR (and from other kinds of privacy regulation) cease to grant data subjects control rights of any kind – this is what makes anonymization a tempting way to go for undertakings. Yet, legal protection might in many cases still be necessary for privacy reasons. When exactly data are effectively anonymized is oftentimes difficult to determine, both from a factual/technical and from a legal point of view. Furthermore, it is rather easy for data controllers to claim that they have anonymized datasets in an effective manner. The latter is very hard, if not impossible to probe for authorities and users alike. Re-identification might just be discovered when it is already too late and serious privacy breaches have occurred. Thus, privacy is at stake as significantly more disclosure of information may take place than data subjects might reasonably expect. Furthermore, their hands are tied in that they cannot do anything against "their" poorly anonymized data being, for instance, sold and transferred to third parties, and in most situations they do not even know about this in the first place. As such, a desirable balance between privacy and disclosure is not always given.

that would be considered "personal data" under the GDPR are freely available to the public in the US in comparison to EU countries.

[135] Peppet S. R. (2014), "Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security, and Consent" 93(1) *Texas Law Review:* 85, p. 130.

[136] *Ibid.*

3.2. The boundaries of EU competition law enforcement vis-à-vis exploitative abuses

3.2.1. "Filtering" competition law intervention vis-à-vis excessive and discriminatory pricing

Economists are traditionally skeptical *vis-à-vis* competition law intervention against excessive and discriminatory pricing. Besides the risk of price regulation caused by the NCA intervention and the overlap with sector regulation, economists are generally confident that in the long run the market could self-adjust and the exploitative conduct would disappear. In other words, if the price of the product is indeed too high and discriminatory, consumers will either stop buying the product or they will switch to another supplier. [137] Finally, "…according to the conventional wisdom, excessive pricing should not be enforced in technological markets because high prices, and hence high profits, are necessary to reward innovation". [138]

A number of economists, however, recognize that in exceptional circumstances EU competition law could sanction excessive pricing. [139] In particular, a number of economists have elaborated a number of "filters" to limit the scope of EU competition policy intervention in this field. [140] It would go beyond the scope of this paper to compare the proposed tests in a systematic manner. [141] However, it is worth mentioning what the common criteria are that economists generally accept "to filter" competition policy intervention *vis-à-vis* excessive pricing:

1) High and non-transitory entry barriers: economists recognize that competition policy should sanction excessive pricing only in markets characterized by high entry barriers. The latter can be either structural (e.g. presence of a network) or legal (e.g. a

[137] Hubert P., Combet M.-L. (2011), "Exploitative Abuse: the End of the Paradox?" 1 *Concurrences*: 51.
[138] *Ibid*.
[139] In support of this view are, for instance, Ezrachi A., Gilo D. (2008), "Are Excessive Prices Really Self-Correcting?" 5(2) *Journal of Competition Law and Economics*: 249-268.
[140] See, in particular, the following contributions in the volume published by the Swedish Competition Authority on excessive pricing: *Konkurrensverket* (Swedish Competition Authority, ed.), *The Pros and Cons of High Prices* (Stockholm, Lenanders Grafika, 2007), available at http://www.konkurrensverket.se/globalassets/english/research/the-pros-and-cons-of-high-prices-14mb.pdf (22.5.2018):
- Motta M., De Streel A., "Excessive Pricing in Competition Law: Never Say Never?"
- Lyons B., "The Paradox of the Exclusion of Exploitative Abuse".
[141] For an exhaustive analysis of the economics literature on competition policy intervention *vis-à-vis* excessive pricing see: OECD Secretariat Background Note, *Excessive Prices.* (Paris, 7.2.2012). The text of the report is available at: https://www.oecd.org/competition/abuse/49604207.pdf (22.5.2018).

dominant company has an exclusive monopoly right to operate in the market).[142] In particular, the entry barriers should be non-transitory. As pointed out by Fletcher and Jardine, NCAs should limit their intervention to cases where entry of new firms is very unlikely in the near future.[143]

2) Super-dominance: in view of the high entry barriers, the dominant company enjoys a super-dominance/quasi monopoly position within the relevant market. Economists generally agree that the traditional 40% market share to justify competition law intervention *vis-à-vis* exclusionary practices would be "too low" to serve as a threshold in the case of excessive pricing.

3) Absence of sector regulation: since high entry barriers and the subsequent super-dominance are common scenarios in network industries (e.g. electricity, gas, railway), a number of economists have argued that EU competition law should sanction excessive pricing in these industries only in the lack of sector regulation.[144] In other words, if the National Regulatory Authority (NRA) regulates the prices, an NCA should not intervene.

4) Hampering innovation: a number of economists have elaborated additional criteria to those mentioned above. In particular, Evans and Padilla argue that EU competition law intervention is justified only if excessive pricing obstacles the introduction of a new product in the market.[145] Similarly, O'Donoghue and Padilla argue that competition policy should not sanction the excessive price of a product covered by a patent, in order to safeguard the patent holder's incentives to innovate.[146]

If we analyse these criteria in the light of the CJEU case law discussed in section 2, we notice that the first two conditions are also followed in the jurisprudence of the Court of Luxembourg. In the cases analysed in section 2, in fact, the dominant company either enjoyed a legal monopoly right (e.g. *Latvian Copyright Society*) or it had a super-dominant position due to the high structural barriers in the industry (e.g. United Brands was the main importer of bananas in

[142] Cf. *supra*, Motta/De Streel.
[143] A. Fletcher A. Jardine (2008), "Towards an Appropriate Policy for Excessive Pricing" in Ehlermann C. D., Marquis M. (eds.), *European Competition Law Annual: 2007 – a Reformed Approach to Art. 82 EC* (Hart Publishing, Oxford), p. 533-546.
[144] See, for instance, *supra*, Motta/De Streel (2007).
[145] Evans D., Padilla J. (2004), "Excessive Prices: Using Economics to Define Administrable Legal Rules" CEMFI Working Paper No. 416. The paper is available at http://www.cemfi.es/ftp/wp/0416.pdf (22.5.2018).
[146] O'Donoghue R., Padilla J. (2006), *The Law and Economics of Article 82 EC* (Hart Publishing, Oxford).

Europe and entry in the market was very unlikely). Super-dominance and high entry barriers are "filters" that the Court of Luxembourg and the EU Commission have followed in relation to the other exploitative conducts, too. In particular, in the majority of cases discussed in sections 2.2 and 2.3 the dominant firm enjoyed a legal monopoly, either by managing a sea harbour (i.e. *Corsica Ferriers* and *Porto di Genova)* or as a collective copyright society (i.e. *MEO, GVL* and *BRT)* or by enjoying an exclusive right to distribute a product in the country (i.e. *Irish Sugar, AAMS).* Therefore, we conclude that even if neither the EU Commission nor the Court of Luxembourg have ever recognized *de iure* that they would sanction exploitative conducts under Art. 102 TFEU only in the presence of very high entry barriers and super-dominance, *de facto* this is the enforcement policy that has been followed by the EU institutions since the Treaty of Rome. The acceptance of these two filters by the EU institutions explains why Art. 102 TFEU has been relied on only in exceptional circumstances to sanction exploitative conducts.

In his opinion in *Latvian Copyright Society,* AG Wahl argued that EU competition policy should sanction excessive pricing only in the presence of high entry barriers and, in particular, that "…unfair prices under Art. 102 TFEU can only exist in regulated markets".[147] According to the AG, in regulated markets the NRA could solve the issue of excessive pricing via *ex ante* price regulation; only in case of a "regulatory failure" by the NRA, antitrust intervention should solve the excessive pricing issue.[148] AG Wahl thus supported the third criterion mentioned above (i.e. antitrust intervention can sanction excessive pricing only in the absence of sector regulation). Nevertheless, in its final judgement the CJEU did not follow the AG's opinion on this point. The Court did not introduce any filter in relation to the application of EU competition policy to sanction excessive pricing.[149] The judgement reflects the traditional Court's view, whereby the presence of sector regulation does not prevent the enforcement of EU competition law. For instance, in *Deutsche Telekom* the CJEU upheld the EU Commission's decision whereby Deutsche Telekom had abused its dominant position by undertaking a margin squeeze strategy that hampered its competitors.[150] In

[147] AG's opinion in case C-177/16, *Autortiesību un komunicēšanās konsultāciju aģentūra v. Latvijas Autoru apvienība v Konkurences padome* (2017) ECLI:EU:C:2017:286, para. 48.
[148] *Ibid.*, para. 49.
[149] In the final judgment, the CJEU simply ruled that "the abuse of a dominant position within the meaning of that article might lie in the imposition of a price which is excessive in relation to the economic value of the service provided", by thus avoiding to introduce any "filter" to the application of EU competition policy *vis-à-vis* excessive pricing.
Supra, Case C-177/16, para. 35.
[150] Case C-280/08, *Deutsche Telekom v. Commission* (2010) ECLI:EU:C:2010:603, para. 80-85.

particular, the Court rejected Deutsche Telekom's arguments that there was no breach of Art. 102 TFEU because the German telecom regulator had approved the interconnection tariff at the origin of the margin squeeze.[151] Transposing *Deutsche Telekom* case law to exploitative abuses, we could argue that the NCA enforcement action *vis-à-vis* an exploitative conduct would be independent of the presence or absence of sector regulation: EU competition law pursues goals that are different from sector regulation and thus its enforcement cannot be prevented by a concurrent legal regime.

The last filter has a clear impact on technology markets, but in our view it seems too restrictive: excessive prices may harm customers and final consumers, even if they do not discourage innovation or prevent the introduction of a new product in the market. In addition, avoiding competition law intervention *vis-à-vis* excessive pricing linked to a patent right, as suggested by O'Donoghue and Padilla, could actually discourage innovation. As recently recognized by Kai-Uwe Kühn, in fact, the hold-up of a standard essential patent (SEP) might cause excessive pricing in terms of high royalty rates demanded by the patent holder to the implementer.[152] According to Kühn, such kind of practice could be tackled via competition law enforcement. Finally, the Court of Justice has never ruled that Art. 102 TFEU should be enforced only *vis-à-vis* exploitative conducts that harm innovation.

To sum up, in our opinion the first two filters should guide the EU Commission's and NCAs' enforcement when it comes to prosecuting exploitative conducts in the data economy. Although they are not legally binding, they reflect the traditional approach followed by EU institutions to limit the enforcement of Art. 102 TFEU against exploitative conducts to exceptional cases; cases characterized by high entry barriers and super-dominance. Online platforms might be super-dominant, due to the large quantity of personal and machine data they control. Furthermore, direct and indirect network externalities often represent high entry barriers that discourage new operators from entering into the relevant market. Therefore, there are good reasons to argue that rather than "filtering" competition law intervention in data markets, the first two criteria actually justify EU competition policy intervention in sanctioning exploitative conducts by super-dominant

[151] By referring to the special responsibility of the dominant company not to breach Art. 102 TFEU, the CJEU ruled an undertaking is not liable for a breach of EU competition law when its market conduct is determined by national law. However, an undertaking was liable if the legislation "merely encouraged" the anti-competitive conduct. In this case, Deutsche Telekom was free to determine the retail price of its internet services. Therefore, it could increase its retail prices in order to avoid margin squeeze.
Ibid., para. 80-85.

[152] Kühn, K.-U. (2017), "Exploitative Abuse: When Does Enforcement Make Sense?" 2 *Concurrences*: 1-3.

online platforms. By contrast, the third and the fourth criteria seem too far-reaching and find no support in CJEU case law.

3.2.2. Competition, data protection and consumer law: what route shall we take?

The market failures in the data economy discussed in section 3.1 open the issue of the interaction of competition, data protection and consumer law. This is a general problem that affects the enforcement of EU competition law in the data economy. This issue, however, is particularly relevant in relation to the application of EU competition law to unfair contractual clauses in the context of the data economy. A number of authors, in fact, have argued that competition law is not the most suitable legal instrument to sanction unfair clauses imposed by online platforms on final users; the latter, in fact, could rather be sanctioned either via consumer or data protection law.[153] In this section we discuss these concerns by comparing the objectives, scopes of application and systems of enforcement of competition, data protection and consumer law.

Competition, data protection and consumer law share the overarching aim of protecting the welfare of individuals in the modern market economy.[154] In particular, these fields of law are concerned with the power asymmetry between individuals and undertakings.[155] In spite of these "family ties", the objectives, scopes of application and enforcement regimes of each policy are rather different.[156] In terms of goals, during the past decade EU competition law has recorded a progressive shift from the objective of safeguarding undistorted competition within the EU internal market to the protection of consumers' welfare.[157] In particular, by sanctioning the anti-competitive behaviour of undertakings, competition policy indirectly safeguards the aggregate welfare of consumers.[158] The

[153] See for instance:
- Ohlhausen M., Okuliar A. (2015), "Competition, Consumer Protection and the Right Approach to Privacy" 80(1) *Antitrust Law Journal:* 121-156.
- Manne G., Sperry B. (2015), "The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework" 2 *CPI Antitrust Chronicle*: 2-11.
- Colangelo G., Maggiolino M. (2017), "Data Protection in Attention Markets: Protecting Privacy through Competition?" 8(6) *Journal of European Competition Law and Practice:* 363-369.

[154] Costa-Cabral F., Lynskey O. (2017), "Family Ties: the Intersection between Data Protection and Competition in EU Law" 54 *Common Market Law Review:* 21.

[155] *Ibid.*, p. 22.

[156] *Ibid.*, p. 14.

[157] Decker C. (2017), "Concepts of the Consumer in Competition, Regulatory and Consumer Protection Policies" 13(1) *Journal of Competition Law and Economics:* 162.

[158] *Ibid.*

scope of application of EU competition law is horizontal: this field of law is applicable to private and State owned undertakings, as well as to public entities when they operate in the market.[159] The core provisions of EU competition law have been primary law since the Treaty of Rome:[160] since the decentralization of EU competition law, in fact, the EU Commission and NCAs enforce Art. 101 and 102 TFEU in parallel.[161] In addition, national courts have a growing role in private enforcement of competition law.[162]

Data protection law safeguards the privacy rights of individuals as "data subjects", as well as the "free movement of personal data".[163] Data subjects can be consumers when data protection affects the processing of personal data by private firms, but they can also be citizens who interact with the public administration.[164] In terms of application, data protection has a different scope than competition law, since its approach is different: it is only applicable to "personal

[159] Art. 106(1) TFEU extends the scope of application of EU competition rules to State owned undertakings and public entities operating in the market: "In the case of public undertakings and undertakings to which Member States grant special or exclusive rights, Member States shall neither enact nor maintain in force any measure contrary to the rules contained in the Treaties, in particular to those rules provided for in Article 18 and Articles 101 to 109."

[160] Art. 101 TFEU sanctions anti-competitive agreements, while Art. 102 TFEU sanctions abuses by dominant companies. The text of these two provisions has not changed since the Treaty of Rome in 1957.

[161] Art. 35(1) Reg.1/2003 required EU Member States to designate a National Competition Authority in charge of enforcing Art. 101-102 TFEU. Although Reg.1/2003 did not harmonize the powers and the institutional structure of the NCAs, every Member State has established an administrative or a judicial authority in charge of enforcing EU competition law at the national level.
Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty. OJ L-1/1, 4.1.2003. Art. 35(1).

[162] National civil courts of the EU Member States have jurisdictions to hear damage and injunction cases linked to breaches of Art. 101-102 TFEU. The 2014 Damages Directive has partially harmonized for the first time the national procedural rules applicable to damage cases in EU competition law.
Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union. OJ L-349/1, 5.12.2014.

[163] Art. 4(1) GDPR defines the data subject as "…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".

[164] The GDPR applies to the "processing of personal data wholly or partly by automated means" (Art. 2(1)), "…the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not" (Art. 3(1)). The GDPR, therefore, has the same scope of application *vis-à-vis* personal data processed by State authorities and public undertakings. However, activities concerning public security, matters of criminal prosecution etc. fall outside the scope of the GDPR (Art. 2(2)(d) GDPR).

data" that reveal information about the identity of the data subject. As discussed in section 3.1.7, data fall outside the scope of data protection regulation both in case of effective anonymization, and when data have never been "personal" from the outset (such as weather data or many kinds of machine data).[165] Similarly to competition policy, the core provisions of data protection law are primary law within the EU legal system. In particular, since the Treaty of Lisbon data protection is recognized as a fundamental right in the EU Charter of Fundamental Rights.[166] Similarly to competition law, the system of enforcement of this policy has been decentralized: national supervisory authorities are the main enforcers of the new General Data Protection Regulation (GDPR).[167] On the other hand, unlike competition policy, an EU-wide data protection agency does not exist.[168] Private enforcement also takes place, but to a lesser extent than in competition law matters.

The objective of consumer law is to safeguard the informed free choice of consumers. Unlike competition law, consumer law protects the welfare of individual consumers, rather than the aggregate consumers' welfare in the economy.[169] Instead of sanctioning the anti-competitive behaviours that have an indirect negative impact on the welfare of final consumers, consumer law sanctions unfair contractual terms that could mislead consumers and thus harm their free choice.[170] In terms of scope of application, consumer law covers the contractual relationship between undertakings and final consumers, while business-to-business relationships fall outside the scope of this policy.[171] Similarly to data protection, a right to a high standard of consumer protection has also been included in the EU Charter of

[165] Oostveen M. (2016), "Identifiability and the Applicability of Data Protection to Big Data" 6(4) *International Data Privacy Law:* 299-309.

[166] Art. 8 EU Charter of Fundamental Rights introduces for the first time an explicit general right of protection of personal data for EU citizens (Charter of Fundamental Rights of the European Union, OJ C-326/391, 26.10.2012).

[167] Art. 51 GDPR requires every EU Member State to establish an independent supervisory authority, in charge of enforcing the GDPR. In particular, the GDPR harmonizes the enforcement powers of the supervisory authorities and it introduces mechanisms of cooperation in cross-border cases.
Cf. Chapters VI and VII of the GDPR.

[168] The European Data Protection Supervisor (EDPS), in fact, has a limited task: it ensures the compliance with data protection rules by the EU institutions. While in competition policy, the European Commission has the task of coordinating the investigations conducted by NCAs and it can directly investigate cross-border cases under Art. 101-102 TFEU, under the EU data protection regime no EU institution has a similar enforcement role.
For further information about the EDPS see: https://edps.europa.eu/ (22.5.2018).

[169] OECD Secretariat Background Note, "The Interaction and Coordination of Competition Policy and Consumer Policy: Challenges and Possibilities" Document published on 5.6.2008, DAF/COMP/GF(2008)10, para. 3.1.

[170] Albors-Llorens A. (2014), "Competition and Consumer Law in the European Union: Evolution and Convergence" 33(1) *Yearbook of European Law*: 169.

[171] *Ibid.*

Fundamental Rights.[172] Nevertheless, the consumer law *acquis* is less harmonized at the EU level than competition and data protection law in terms of secondary legislation. During the past decades, the EU has adopted a number of Directives to harmonize national consumer law.[173] However, differences still persist at the national level, in particular in relation to the enforcement regime:[174] while some Member States have established an administrative authority in charge of enforcing the EU consumer law *acquis,*[175] other Member States rely on a judicial system of redress.[176]

---

[172] Art. 38 EU Charter of Fundamental Rights provides that "the Union shall ensure a high level of consumer protection".

[173] The core EU consumer law *acquis* is represented by Directive 2005/29/EC, providing an harmonized list of unfair business-to-consumer commercial practices, and the Directive 2011/83/EU, which consolidates in a single legislation the consumers' rights previously included in different Directives.

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

Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council. OJ L-304/64, 22.11.2011.

[174] Regulation 2006/2004/EC introduced forms of cooperation and exchange of information among national authorities involved in cross-border consumer law cases. However, unlike data protection and competition law, Regulation 2006/2004/EC did not require the EU Member States to establish a national administrative authority in charge of enforcing the consumer law *acquis.*

Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation), OJ L-364/1, 9.12.2004.

[175] In Italy, the Legislative Decree transposing the Unfair Commercial Practices Directive 2011/83/EU granted to the Italian Competition Authority (*Autorità Garante per la Concorrenza e il Mercato*) the power to impose administrative fines on companies that carry out unfair commercial practices damaging consumers. Since 2007, the Italian Competition Autorità enforce the consumer law *acquis* in parallel to competition law.

Attuazione della direttiva 2005/29/CE relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica le direttive 84/450/CEE, 97/7/CE, 98/27/CE, 2002/65/CE, e il Regolamento (CE) n. 2006/2004. Italian Legislative Decree n. 146, adopted on 2.8.2007. The text of the legislation is available at: http://www.agcm.it/normativa/consumatore/4526-decreto-legislativo-2-agosto-2007-n-146-pratiche-commerciali.html (22.5.2018).

[176] For instance, Germany follows a system of judicial redress in the field of consumer law. The *Gesetz zur Umsetzung der Verbraucherrechterichtlinie und zur Änderung des Gesetzes zur Regelung der Wohnungsvermittlung* implemented in 2013 the Consumer Rights Directive 2011/38/EU. Consumers can enforce their rights either via court proceedings or via alternative systems of redress (ADR – e.g. arbitration, mediation etc.). At the moment, there is no public authority in Germany in charge of adopting administrative decisions to enforce the consumer law *acquis.*

This brief overview of the objectives, scopes of application and enforcement regimes shows that these three policies share a number of common features (i.e. "family ties"). At the same time, the differences demonstrate that these policies cannot replace each other. They co-exist since they pursue different goals via different tools, and they have a different scope of application respectively. Therefore, as argued in 2014 by the European Data Protection Supervisor, the three policies should "dialogue" in the context of the data economy.[177] However, data protection and consumer law cannot prevent *a priori* the enforcement of EU competition law in the data economy. The same view was also expressed in 2016 by the German *Bundeskartellamt* and the French *Autorité de la Concurrence* in their joint report on competition law enforcement in the data economy:

"the fact that some specific legal instruments serve to resolve sensitive issues on personal data does not entail that competition law is irrelevant to personal data. Generally speaking, statutory requirements stemming from other bodies of law may be taken into account, if only as an element of context, when conducting a legal assessment under competition law."[178]

Gesetz zur Umsetzung der Verbraucherrechterichtlinie und zur Änderung des Gesetzes zur Regelung der Wohnungsvermittlung, adopted on 20.9.2013, BGBl I S. 3642. The text of the legislation is available at: http://www.bundesgerichtshof.de/DE/Bibliothek/GesMat/WP17/V/VerbraucherrechteRL.html (22.5.2018).

[177] In March 2014, the European Data Protection Supervisor (EDPS) published a preliminary opinion on the interplay between competition, data protection and consumer law in the contest of the digital economy. The report called for more coordination among the enforcement authorities of the 3 policies in cases affecting the data economy. The 2014 report was followed by a EDPS opinion released in September 2016; opinion that further discuss the mechanisms of coordination among the enforcement authorities of 3 policies.

European Data Protection Supervisor preliminary opinion, "Privacy and Competitiveness in the Age of Big Data: the Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy" (published in March 2014). The preliminary opinion is available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-and-competitiveness-age-big-data_en (22.5.2018).

European Data Protection Supervisor, "EDPS Opinion on Coherent Enforcement of Fundamental rights in the Age of Big Data", Opinion 8/2016, published on 23 March 2016. The opinion is available at: https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf (22.5.2018).

For a comment of the 2014 EDPS preliminary opinion, see Costa-Cabral F. (2016), "The Preliminary Opinion of the European Data Protection Supervisor and the Discretion of the European Commission in Enforcing Competition Law", 23(3) *Maastricht Journal of European and Comparative Law:* 495-513.

[178] Joint report of the German *Bundeskartellamt* and the French *Autorité de la Concurrence*, "Competition Law and Data", published on 10 May 2016, p. 23. The text of the report is available at: http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/10_05_2016_Big%20Data%20Papier.html (22.5.2018).

The same view is also confirmed by CJEU case law. In particular, in *Asnef-Equifax* the Court ruled that "…any possible issues relating to the sensitivity of personal data are not, as such, a matter of competition law, they may be resolved on the basis of the relevant provisions governing data protection."[179] This *obiter dictum* should not be read as an *a priori* prevention of EU competition law enforcement in matters overlapping with data protection law. *Asnef-Equifax* should rather be read as recognition that competition, data protection – and consumer – law are separate policy areas that pursue different objectives. On the one hand, competition law should aim at solving market failures and safeguarding consumer welfare, rather than tackling privacy violations affecting the data subjects. On the other hand, it would be up to the enforcement authority (i.e. EU Commission/NCAs) to decide when data protection and consumer law cannot effectively tackle the market failures analysed in section 3.1, and thus EU competition law should intervene. This view is confirmed by *Deutsche Telekom* judgement, where the legality of the firm's conduct under telecom regulation did not prevent the EU Commission from sanctioning the undertaking for abuse of a dominant position.[180] Similarly, in *Astra Zeneca* the Court ruled that the "…illegality of abusive conduct under [now: Art. 102 TFEU] is unrelated to its compliance or non-compliance with other legal rules and, in the majority of cases, abuses of dominant positions consist of behaviour which is otherwise lawful under branches of law other than competition law."[181]

To sum up, competition, data protection and consumer law share a number of "family ties"; ties that are particularly evident in the context of the data economy. Although these policies share common aims, they have different objectives, scopes of application and enforcement regimes. As confirmed by the CJEU case law, the legality of a conduct under another legal regime does not prevent the enforcement of EU competition law. While in the context of the data economy EU competition law should not pursue data protection goals, competition law enforcers should have the discretion to intervene in case of market failures in the data economy, even in the presence of overlapping data protection and consumer law applicability.

[179] Case C-238/05, *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v Asociación de Usuarios de Servicios Bancarios* (2006) ECLI:EU:C:2006:734, para. 63.
[180] *Supra*, Case C-280/08, para. 80-85.
[181] Case C-457/10, *AstraZeneca AB and AstraZeneca plc v. European Commission* (2012) ECLI:EU:C:2012:770, para. 132.

4. Exploitative conducts in the data economy

In this section we continue our exploration of the *terra incognita* by analysing specific exploitative conducts in the context of the data economy; conducts that may harm consumers/customers of the dominant company, rather than to exclude competitors. In particular, we discuss the role of Art. 102 TFEU in sanctioning excessive pricing, behavioural discrimination, as well as unfair contractual clauses applied by dominant online platforms *vis-à-vis* their users. After an overview of the technical aspects of these abuses in the context of the data economy, we analyse the application of Art. 102 TFEU by looking at the CJEU case law discussed in section 2, as well as at the findings of section 3 concerning the scope of application of EU competition law in the data economy.

In this section, we analyse the potential challenges that the EU Commission and NCAs would face in satisfying the criteria elaborated by CJEU case law in order to enforce Art. 102 TFEU *vis-à-vis* exploitative conducts in data markets. While the discussion on excessive pricing (i.e. section 4.1) and behavioural discrimination (i.e. section 4.2) is rather "theoretical", since there have not been any enforcement cases (yet), section 4.3 analyses unfair contractual terms in the data economy in light of the recent *Facebook/WhatsApp* merger case, as well as the on-going investigations conducted by the *Bundeskartellamt* in the *Facebook* case.

As mentioned in the introduction, in this paper we do not discuss issues related to the relevant market definition and market power. We take for granted that the online platform has substantial market power, and thus we analyse possible exploitative abuses under Art. 102 TFEU. The discussion in section 4 represents the departing point of the final part of our journey in the *terra incognita*: in section 5 we will analyse possible EU competition law remedies to solve the exploitative conducts identified in section 4.

4.1. Excessive pricing in the data economy

4.1.1. Excessive pricing *vis-à-vis* final consumers – the problem of the counter-performance

As discussed in section 3.1, a peculiarity of the data economy is that online users often receive "free" services from online platforms: apps, videos, games, maps, search engines etc. are freely provided to internet users "in exchange" for their personal data.[182] In other words,

[182] Langhanke C., Schmidt-Kessel M. (2015), "Consumer Data as Consideration" 6 *Journal of European Consumer and Market Law*: 218.

the users agree to "reduce" their privacy in exchange for some kind of service. The online platform will use the large amount of data collected to create detailed consumer profiles, either to improve the marketing of its products or to sell such precious information to other firms.[183]

The EU Commission has recognized this new business model that characterizes the data economy in its 2015 Directive proposal on the sale of digital content.[184] The Council and the European Parliament have not approved this legislation yet, and thus it has not entered into force.[185] Nevertheless, the scope of this legislation is an interesting aspect of the proposal: the draft Directive recognizes for the first time that personal and non-personal data may represent a "counter-performance" in a contract concluded between an online platform and an internet user.[186]

The debate on the nature of the counter-performance could be relied on in the discussion on sanctioning excessive pricing in the data economy. In a world where platforms mainly provide "free" services to final consumers, in fact, the traditional concept of excessive pricing requires an update. As discussed in section 2.1, since *United Brands* the CJEU has consistently defined excessive pricing as an "unreasonable" price in comparison to the economic value of the product purchased.[187] If we rely on this definition in the context of the data economy, Art. 102 TFEU could sanction the excessive amount of personal data that a dominant online platform requests from internet users. In view of the *Latvian Copyright Society* case law, the benchmark to determine if the amount of data requested by the dominant platform is "excessive" could be the personal data requested by other online platforms for the provision of a similar

[183] In relation to the discussion of the effective "price" paid by consumers to get access to "free" online services see:
- Stacy-Ann E. (2017), "Paying for Privacy and the Personal Data Economy" 6 (117) *Columbia Law Review:* 1369.
- Gal M., Rubinfeld D. (2016), "The Hidden Costs of Free Goods: Implications for Antitrust Enforcement" 80 *Antitrust Law Journal:* 401.

[184] European Commission, Proposal for a Directive of the European Parliament and of the Council on Certain Aspects concerning Contracts for the Supply of Digital Content. Brussels 9.12.2015, COM (2015)634 final.

[185] At the moment of writing, the proposal has been debated both in the Council and in the European Parliament. However, due to the different positions of the two institutions on the proposal, in November 2017 the European Parliament voted to open inter-institutional negotiations with the Council to achieve a compromise on a shared legal text. Updated information on the steps in the approval of the legislative proposal are available on the Legislative Observatory of the European Parliament. http://www.europarl.europa.eu/oeil/home/home.do (22.5.2018).

[186] "The Directive shall apply to any contract where the supplier supplies digital content to the consumer or undertakings to so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data." (Art. 3(1) Directive Proposal).

[187] *Supra*, Case 27/6, para. 250.

online service.[188] The difference in terms of quality and amount of data requested by other online platforms would have to be "consistent" and "persistent".[189] Finally, it would be up to the online platform to put forward justifications.[190] For instance, the dominant operator could argue that it provides a "better" service than its competitors, which in turn justifies a larger amount of personal data provided by final consumers as counter-performance.

If "in theory" sanctioning the excessive request of personal data under Art. 102 TFEU would be possible, "in practice" an NCA would face a number of enforcement challenges that are truly *incognite*. First of all, privacy preferences are highly subjective: it would be quite difficult for an NCA to determine when the amount/quality of personal data requested by the online platform is truly "excessive".[191] Secondly, *Latvian Copyright Society* refers to "consistent" and "persistent" disparities: vague terms that would leave a broad margin of discretion to the NCA, and they would imply a high risk that the NCA decision is annulled by a court on appeal. Secondly, the online platform could put forward good arguments to justify its conduct: if consumers are willing to transfer certain personal data to the online platform, they implicitly accept the value of the service offered by the online platform in comparison to the amount of data requested as counter-performance. In other words, it would be hard for the NCA to estimate the extent of the "privacy paradox" when assessing the amount of data requested by the online platform. Finally, as discussed in section 3.2.1, the EU Commission and NCAs have usually sanctioned cases of excessive pricing in markets characterized by super-dominance and high entry barriers; these conditions have also been followed in CJEU case law. Although data markets may give rise to cases of super-dominance, it would be hard to argue that digital markets have high and stable entry barriers to justify competition law intervention *vis-à-vis* a super-dominant online platform.

In view of these considerations, no NCA has ever sanctioned any case of excessive pricing in data markets. The *Facebook* investigations carried out by the *Bundeskartellamt* and the *Facebook-WhatsApp* merger case discussed in section 4.3 are examples of unfair contractual clauses in data markets, rather than cases involving excessive pricing. Therefore, we will probably have to wait for some

[188] *Supra*, Case C-177/16.
[189] *Supra*, Case C-177/16, para. 55.
[190] *Supra*, Case C-177/16, para. 58.
[191] A number of studies in the field of behavioural economics have tried to estimate the consumers care about online privacy. However, the results of such studies are quite divergent. For a comparative view on the behavioural economics studies on consumers online privacy, see Kokolakis S. (2017), "Privacy Attitudes and Privacy Behaviour: a Review of Current Research on the Privacy Paradox Phenomenon" 64 *Computers and Security:* 122-134.

time before a competition law enforcer explores this area of the *terra incognita.*

4.1.2. Excessive pricing *vis-à-vis* industrial customers – access to the database as an essential facility

While it is unlikely that Art. 102 TFEU may be relied on in the future to sanction the excessive amount of personal data requested by an online platform from its users, the situation would be different in case of industrial customers; for instance, when it comes to industrial customers willing to pay a price to access a database held by a dominant provider. In such a scenario, the counter-performance would be a "traditional" monetary counter-performance, rather than (personal) data. The dominant provider could be either a search engine, or a social network, or a data broker that has collected a number of information and has systematized these data in order to sell them on the market.[192] In principle, the "excessive" access price charged by a dominant platform could be sanctioned under Art. 102 TFEU, even in the absence of any exclusionary intent by the dataset provider. In view of the *Latvian Copyright Society* decision, the benchmark of comparison would be the access price charged by other data providers for similar datasets, taking into consideration the quality and quantity of the data made available. The price disparity would have to be "consistent" and "persistent" in order to be sanctioned under Art. 102 TFEU. Finally, the dominant company could argue that the "excessive" access price is justified by the better quality of its dataset.

This type of enforcement of Art. 102 TFEU would also open a number of *incognite*. First of all, the comparison with "similar" databases would be a complex task, taking into consideration the rapid degradation of the data value and the subjective nature of data quality for marketing and other purposes. The comparison would become almost impossible when real-time data are concerned (i.e. a constant flow of information), which is nowadays oftentimes the case. Secondly, it would be hard to estimate if the price difference is "consistent" and "persistent" – i.e. a general excessive pricing policy by the dataset provider, rather than an isolated case. Yet, the privacy paradox would not affect the NCA's assessment of this type of cases: the NCA assessment would rather follow the traditional CJEU case law on excessive pricing, especially *Latvian Copyright Society*.

[192] OECD Secretariat, *Data-Driven Innovation. Big Data for Growth and Well-Being.* Report published on 6.10.2015, p. 34. The text is available at: http://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm (22.5.2018).

Finally, the traditional "filters" (super-dominance of the online platform and high entry barriers in the market) would be applicable in case of excessive access pricing charged by a dataset provider. In this context, the database could be considered an "essential facility". From this point of view, the conditions identified by CJEU case law in *IMS Health* to determine when access to a database is "essential" could be applied to this case: [193] access to the database would be "indispensable" to offer a "new product" in the downstream market; the replication of the database is "impossible"; the dominant firm cannot put forward any "objective justification". The essential facility doctrine has been elaborated by the CJEU case law as an abuse concerning a refusal to deal – i.e. an exclusionary conduct by the owner of the essential facility.[194] However, such conditions could also be relied on in case of excessive pricing to determine whether the relevant market is characterized by high entry barriers – i.e. when the database becomes "essential" since there is no other provider in the market. It is well known that these conditions are rather "strict" and difficult to satisfy in practice.[195] As argued by Colangelo and Maggiolino, it would be hard to satisfy the "impossibility" and "indispensability" requirements in the case of big data.[196] Since personal data is an "abundant" raw material in the modern data economy, in principle it would be difficult to argue that a dataset cannot be replicated.[197] From a legal point of view, the dominant online platform would not have an exclusive right on the data collected since multi-homing is possible in the data economy. A new entrant would thus be free to collect the same data from the same users.[198] In addition, from a technical point of view, a new entrant could buy a dataset from a data broker if it does not have the infrastructure to directly collect and process the data itself.[199] Thus, the "impossibility" condition would be satisfied only in exceptional cases (i.e. the dominant online platform enjoys a legal monopoly to collect and process data).[200] Finally, in terms of "indispensability", it

[193] Case C-418/01, *IMS Health GmbH & Co. OHG v. NDC Health GmbH & Co. KG*. (2004) ECLI:EU:C:2004:257.

[194] Besides the *IMS Health* case, see the ruling of the Court of Justice in *Oscar Bronner* and the judgement of the General Court in *Microsoft.*

Case C-7/97, *Oscar Bronner GmbH & Co. KG v. Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint* (1998) ECLI:EU:C:1998:569.

Case T-201/04, *Microsoft Corp. v. European Commission* (2007) ECLI:EU:T:2007:289.

[195] For instance, in *Oscar Bronner (ibid.)* the applicant failed to satisfy the impossibility condition – i.e. the replication of the facility was costly, but not impossible.

[196] Colangelo G., Maggiolino M. (2017), "Big Data as Misleading Facility" 2(13) *European Competition Journal:* 249-281.

[197] *Ibid.*, p. 255.

[198] *Ibid.*, p. 256

[199] *Ibid.*, p. 259.

[200] *Ibid.*, p.257.

is worth noting that the amount of data held by a platform does not necessarily grant a competitive advantage: data quickly get outdated and their value does not depend on their "quality", but on the way the algorithm can typically infer new information by analysing different pieces of data available.[201] In conclusion, competition law intervention *vis-à-vis* excessive pricing charged by dominant online platforms from industrial customers could take place only in rather exceptional cases.

4.2. Price discrimination in the data economy

4.2.1. Behavioural discrimination in the data economy

Economists traditionally identify 3 degrees of price discrimination:[202]

1) First-degree price discrimination takes place when a firm is able to perfectly discriminate among its customers, adjusting the price of the product to the individual customer's willingness to pay. Thus, in this (mostly hypothetical) scenario the firm would be able to extract the maximum profit on each sale.

2) Second degree price discrimination means that the firm discriminates between its customers by granting discounts once a specific purchase quota is achieved. Second degree price discrimination is usually considered pro-competitive, and it can increase the consumers' welfare. For example, the price of a product might be lower once a specific amount of items is bought at the same time and from the same buyer.

3) Third degree price discrimination takes place when the firm charges different prices to different groups of customers. Third degree price discrimination is rather common in the "real" economy, and it is generally justified by fairness considerations. For example, a movie theatre grants a special tariff to certain categories of "vulnerable" consumers, such as old/retired people or children below a certain age.

First-degree price discrimination has traditionally been considered *de facto* impossible: the seller would not have enough information to

[201] *Ibid.*, p. 256.
[202] For an economic analysis of the anti-competitive effects of price discrimination see:
- Motta M., *Competition Policy – Theory and Practice* (Cambridge University Press, 2004), p. 493-494.
- Varian H., "Price Discrimination" in Schmalensee R., Willig R. D. (eds.), *Handbook of Industrial Organization* (Elsevier Science Publisher, 1989), Chapter 10, p. 597-654.

accurately differentiate the price for each customer. [203] However, as found by a 2015 White House report, big data analytics facilitate the shift from second/third degree price discrimination to first degree price discrimination.[204] Online platforms collect a large amount of personal data via internet cookies, search engines, social platforms etc. These are data relied on by online platforms to create profiles of their customers, in order to understand what types of products consumers are currently searching and thus might be willing to buy.[205] As argued by Maggiolino, big data analytics have radically changed the marketing strategies of the majority of firms.[206] In the past, firms studied the consumers' behaviour by conducting experiments via questionnaires distributed among a small number of people – i.e. a sample of the potential customers of a product.[207] These market studies thus provided an "approximate" view of the behaviour of groups of consumers, and they could be relied on for elaborating marketing strategies. Nowadays, algorithms can process millions of pieces of data, building personal profiles of individual preferences.[208] Via profiling, the platform can analyse a consumer's personality traits and his or her (future) behaviour, and use this knowledge to make him or her buy a certain product by offering either special discounts or purchase conditions (such as an exemption from the payment of the delivery costs); a special price that is not offered to the other customers of the platform. Discriminatory pricing is, thus, a natural consequence of the large amount of personal data collected by online platforms and by the new possibilities offered by data analytics. It is now a common business practice in digital markets, known as "price optimization" or "dynamic differential pricing".[209]

According to Ezrachi and Stucke, first degree price discrimination (i.e. individual pricing) remains unlikely, even in

[203] Geradin D., Petit N. (2006), "Price Discrimination under EC Competition Law: Another Antitrust Doctrine in Search of Limiting Principles?" 2(3) *Journal of Competition Law and Economics:* 485.
[204] Executive Office of the President of the United States, "Big Data and Differential Pricing", published in February 2015, p. 16. The document is available at: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf (22.5.2018).
[205] *Ibid.*, p. 4.
[206] Maggiolino M. (2017), "Personalized Prices in European Competition Law" *Bocconi Legal Studies Research Paper* No. 2984840. The working paper is available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2984840 (22.5.2018).
[207] *Ibid.*, p. 8.
[208] *Ibid.*, p. 8.
[209] Shiller B. R. (2014), "First Degree Price Discrimination Using Big Data", working paper published by the Economics Department of Brandeis University. The paper is available at: http://benjaminshiller.com/images/First_Degree_PD_Using_Big_Data_Jan_27,_2014.pdf (22.5.2018).

digital markets.[210] Although the platform can collect a large number of personal data concerning its users, the platform does not know what the "reservation price" of individual consumers is – i.e. the maximum price that each consumer would be willing to pay for a product; in other words, the price that would maximize the firm's profits.[211] Price discrimination in the data economy rather takes place via different forms of "behavioural discrimination", which represent a mix of the different degrees of discrimination described above. First of all, a search engine could differentiate the list of results shown to different categories of consumers, even though the consumers submitted the same search query (this practice is known as "steering").[212] For instance, Google could assign a higher search ranking to "cheaper" products for consumers oriented to "budget conscious choices", in comparison to the list of products shown to "more affluent" consumers. Secondly, the platform could differentiate the product "decoys" presented to different categories of consumers.[213] For instance, Apple could present a wider range of optional iPhone gadgets to "more affluent" consumers in comparison to the "budget conscious customers", since the latter category of customers would be unlikely to buy additional devices besides the basic model of the product. Thirdly, via "drip pricing" the platform could mislead consumers by showing an initial low price for the product; a price to which the platform automatically "adds on" additional charges before the purchase is finalized.[214] The classical example to this regard is represented by the purchase of airline tickets, where the initial price is usually low to attract the attention of "budget conscious consumers", but additional charges are later added during the purchasing process (e.g. airport taxes, fuel charges, check-in luggage etc.). Finally, the platform could exploit time constraints and willpower of different consumers in order to differentiate the treatment of its customers.[215] For instance, after having searched a type of product on either Amazon or eBay without having concluded the purchase, the platform could contact the potential customer by re-offering the product previously searched at a discounted rate. Consequently, "more patient" consumers usually get better deals when they shop online, in comparison to "less patient" consumers who purchase a product as soon as they find a suitable one. Similarly, the platform could frame special "fake" offers for certain categories of consumers.[216] For instance, coming back to the last example, Amazon or eBay could contact by email the potential customer by offering the product

[210] Ezrachi A., Stucke M., *Virtual Competition* (Harvard University Press 2016), p. 96.
[211] *Ibid.*, p.100.
[212] *Ibid.*, p.107.
[213] *Ibid.*, p. 106.
[214] *Ibid.*, p. 109.
[215] *Ibid.*, p. 110.
[216] *Ibid.*, p. 111.

previously searched at a "special" discounted price; in reality, the original price has been increased meanwhile and thus the discount does not correspond to any real saving for the consumer. Within this scenario, less sophisticated consumers would be more likely to fall within this "trap", by accepting the "special" offer of the platform.

These examples show that online platforms have a large number of tools available to discriminate their customers. Behavioural discrimination relies on consumers' online behaviour, which is "monitored" by online platforms. Besides traditional personal data, such as gender, age, and level of education, other information is essential for online platforms, too. In particular, past online purchases, geo-location, the list of web sites previously visited, as well as search queries are key data that allow online platforms to carry out different forms of behavioural discrimination.

A number of empirical studies have confirmed that behavioural discrimination is already taking place in online markets. For instance, Mikians and others have concluded that "steering" is a common form of behavioural discrimination in online markets.[217] In their empirical study, the authors relied on a number of proxy servers, which simulated search queries originating from different countries in Europe, Asia and the USA. The computers generated synchronized search queries, searching the same product on Amazon and similar marketplaces. The author concluded that the marketplaces generally "steered" users to different products, although the search query was identical, and the search was taking place at the same time on the same web site.[218] In particular, users were "steered" to products dedicated to either "more affluent" or "budget conscious" customers. According to the authors, the discriminatory factors followed by the algorithms were related to the geographic origin of the search query, as well as to the number of personal information concerning the user, such as list of web sites previously visited and purchasing history. On the other hand, the operating system used did not have an impact on the search results. In other words, Mac users were not treated by the platforms as "more affluent" consumers, and thus were not discriminated in comparison to Windows users.[219]

The findings of the study are interesting, since they confirm that behavioural discrimination takes place in digital markets. Nevertheless, they also show the limits of such empirical studies. In

[217] Mikians J. et al., "Detecting Price and search Discrimination on the Internet", conference paper presented at the Universitat Politecnica de Catalunya in October 2012. The text of the paper is available at:
https://www.researchgate.net/publication/232321801_Detecting_price_and_search_discrimination_on_the_Internet
(22.5.2018).
[218] *Ibid.*, p. 1.
[219] *Ibid.*, p. 2.

particular, in order to infer a statistical causality to prove the existence of behavioural discrimination, the authors had to set-up a "large" empirical study, automatically implemented by machines. However, the study was limited to a specific type of behavioural discrimination, namely "steering". Secondly, the findings of the study on the lack of discrimination between Mac and Windows users contradict previous studies on behavioural discrimination.[220] The results of such studies are strongly influenced by the variables taken into consideration and by the study set-up. In particular, it would be hard to prove that an online platform systematically implements behavioural discrimination and that there are no objective justifications to such behaviour. As further discussed in section 4.2.2, the need to prove the systematic nature of discrimination and the possible objective justifications put forward by the online platform are the main reasons why no NCA has so far investigated this type of abuse under Art. 102 TFEU.

The last question discussed in this sub-section concerns the consumers' attitude *vis-à-vis* behavioural discrimination. With the exception of third degree price discrimination justified by fairness considerations, consumers are generally against forms of price discrimination:[221] if a consumer finds out that her or she has paid a higher price for a product in comparison to a friend/relative, he/she will be unlikely to buy again from the same seller. According to Maggiolino, consumers are generally against price discrimination due to the "…fear of being among those who are charged (and pay) more" when purchasing a product, rather than simply due to egalitarian reasons.[222] In addition, an individual price appears "less transparent", since the consumer is not aware of the parameters taken into consideration by the algorithm to calculate the price, even though the price could actually match with the consumer's retention price.[223] These are the main reasons why a number of authors argue that firms do not have an incentive to carry out price discrimination: due to the potentially bad publicity, and thus on their long-term profits.[224] However, as discussed above, empirical studies prove that forms of behavioural discrimination are common in digital markets. Price discrimination is more likely in the data economy in comparison to the "real" economy due to the availability of big data and data analytics.

[220] In an empirical study conducted in 2014, Hannak and others found evidence that the web site Orbitz generally "steered" Mac users towards more expensive hotels in its list results in comparison to the Windows users.
Hannak A., "Measuring Price Discrimination and Steering on E-commerce Web Sites" *Proceedings of the 2014 Conference on Internet Measurement Conference*, p. 305-318. The paper is available at: https://dl.acm.org/citation.cfm?id=2663744 (22.5.2018).
[221] Li K., Jain S. (2014), "Behaviour-Based Pricing: An Analysis of the Impact of Peer-Induced Fairness" 62(9) *Management Science:* 2705-2721.
[222] *Supra,* Maggiolino (2017), p. 12.
[223] *Supra,* Maggiolino (2017), p. 12.
[224] *Supra,* Li/Jain (2014).

Secondly, these forms of discrimination are difficult to be detected: it would be difficult for a consumer to find out that he or she has been "steered" by the platform to buy a more expensive product in comparison to another consumer based in a different country. Therefore, in spite of the consumers' resistance *vis-à-vis* price discrimination, the latter is a common practice in data markets.

The questions discussed in the next section concern the impact of behavioural discrimination on the consumers' welfare, and thus whether and to what extent Art. 102 TFEU could be enforced to sanction behavioural discrimination.

4.2.2. EU competition policy and behavioural discrimination

Economists generally argue that price discrimination is pro-competitive and increases the consumers' welfare; even behavioural discrimination could be pro-competitive. In particular, algorithms could monitor the price offered by competitors and attract their customers by offering better individual rates.[225] Behavioural discrimination would thus strengthen the degree of competition in the market. Furthermore, behavioural discrimination could benefit consumers: the platform could charge a lower price to "budget conscious consumers" who have a lower "retention price", and who are also expected to be "poorer" in terms of personal income. Price discrimination could thus increase the product affordability for a larger number of consumers, and thus facilitate welfare re-distribution among different categories of consumers. [226]

A number of arguments can be put forward against the idea that price discrimination is pro-competitive and increases the consumers' welfare. First of all, price discrimination increases the degree of competition in the market only if the platforms have access to symmetric information about their potential customers.[227] In other words, only if platforms have access to the same information about potential customers they can fiercely compete via individual price offers. In reality, online platforms have access to different categories

[225] In relation to this argument, see for instance:
- Esteves R. B. (2010), "Pricing with Customer Recognition" 28(6) *International Journal of Industrial Organization:* 669-681.
- Esteves R. B. (2014), "Price Discrimination with Private and Imperfect Competition" 31(4) *Scandinavian Journal of Economics:* 634-657.

[226] Geradin D., Petit N. (2006), "Price Discrimination under EC Competition Law: Another Antitrust Doctrine in Search of Limiting Principles?" 2(3) *Journal of Competition Law and Economics:* 479, p. 519.

[227] Choe C. et al. (2017), "Pricing with Cookies: Behaviour-Based Price Discrimination and Spatial Competition", Monash Economics Working Papers 07-17. The paper is available at: https://ideas.repec.org/p/mos/moswps/2017-07.html (22.5.2018).

of personal data concerning individual consumers (i.e. asymmetric information), and thus they cannot target the same customers via target offers.[228]

Secondly, the assessment of price discrimination on consumers' welfare requires a case-by-case analysis, in order to assess the overall impact of price discrimination on the welfare of "richer" and "poorer" consumers.[229] To this regard, it is worth remembering that the objective of price discrimination is to "capture as much consumer surplus as possible"[230]. As argued by Ezrachi and Stucke, the "optimal" price implemented by the online platform is the price where the platform can maximize its profits; the maximum "retention price" that individual consumers are willing to pay for a certain product.[231] Therefore, the "optimal" price shifts part of the consumers' welfare to the online platform: in the absence of price discrimination, in fact, some consumers would pay a lower price for the product in comparison to their retention price. In a nutshell, even if price discrimination could facilitate welfare re-distribution among different categories of consumers, price discrimination is likely to increase the firm's welfare to the detriment of the overall consumers' welfare.

According to Maggiolino, before investigating a case concerning discriminatory pricing, the antitrust authorities should decide whether they protect the total or consumers' welfare.[232] However, consumers' welfare is the accepted standard both under EU competition law and US antitrust law.

In view of these considerations, there is no reason to exclude *a priori* the enforcement of Art. 102 TFEU *vis-à-vis* discriminatory pricing when this practice has an exploitative dimension. Behavioural discrimination is more likely in the context of the data economy, and thus it becomes an issue that should be tackled via EU competition law. A number of questions, however, remain open. First of all, behavioural discrimination could also be tackled under other legislations that prohibit price discrimination.[233] Alternatively, data

[228] *Ibid.*
[229] Bourreau M., De Streel A., Graef I. (2017), "Big Data and Competition Policy: Market Power, Personalised Pricing and Advertising" *Cerre Project Report*, p. 8. The text of the report is available at: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2920301_code485318.pdf?abstractid=2920301&mirid=1 (22.5.2018).
[230] Carlton D., Perloff J., *Modern Industrial Organization* (Addison-Wesley, 1999), p. 280.
[231] *Supra*, Ezrachi/Stucke (2016), p. 96.
[232] *Supra*, Maggiolino (2017), p. 16.
[233] The Robinson-Patman Act is a 1936 US federal legislation that amends the Clayton Act. The Robinson-Patman Act prohibits a seller of commodities from selling comparable goods to different buyers at different prices, except in certain circumstances. The legislation can be enforced by the FTC, which can bring a case

protection law could limit the ability of online platforms to create profiles of their customers. In this regard, it is worth mentioning that the GDPR introduces for the first time a binding definition of "profiling" and puts it in context with automated individual decision-making.[234] Finally, some forms of behavioural discrimination could also be tackled under consumer law. For instance, as argued in the previous section, the online platform could mislead consumers when it automatically adds additional charges before the finalization of the purchase: "drip pricing" could thus be an unfair commercial practice under consumer law.[235]

As argued in section 3.2.2, "alternative routes" do not exclude *a priori* the application of EU competition law to sanction forms of behavioural discrimination. Different regulatory tools have different goals, scopes of application and enforcement regimes. Therefore, the legality of a market behaviour under a certain area of law cannot exclude *a priori* the application of EU competition rules. It is up to the enforcement authority (i.e. the Commission and NCAs) to decide if EU competition law is the most appropriate tool to solve a market failure.

Even if Art. 102 TFEU could sanction in principle behavioural discrimination, a number of factors should also be taken into consideration in terms of EU competition policy enforcement. First of all, the super-dominance and the high-entry barrier "filters" discussed in section 3.2.1 *vis-à-vis* excessive pricing would also be applicable to discriminatory pricing. In particular, in this context the dominant position of the platform would be strengthened by a lack of price comparison web sites. The latter help consumers to compare the offers of different providers. This limits the ability of platforms to discriminate its customers. Secondly, the platform would be super-dominant if it was the main online provider of a category of products within a specific geographic area; an area characterized, for instance, by high entry barriers from a language point of view. In such a context, the consumers would be "locked-in" (i.e. forced to use the

to federal court. Although nowadays the Robinson-Patman Act is rarely enforced in USA, the legislation is still in force.

Robinson-Patman Act, 15 U.S.C.A. § 13(a–f).

[234] Art. 4(4) and 22 GDPR.

In relation to the safeguard of users online profiling in USA, see Steindel T. (2010-2011), "A Path Toward User Control of Online Profiling" 17 *Michigan Telecommunications and Technology Law Review:* 459-490.

[235] For instance, under Art. 6(e) of the Consumers Rights Directive, in distance and off-premises contracts (i.e. like in e-commerce contracts), the seller has to inform the consumer about "the total price of the goods or services inclusive of taxes, or whether the nature of the goods or services is such that the price cannot reasonably be calculated in advance, the manner in which the price is to be calculated, as well as, where applicable, all additional freight, delivery or postal charges and any other costs…"

online platform), and thus behavioural discrimination would be more likely. Obviously, these scenarios are hypothetical as they represent rather extreme scenarios in digital markets.

4.2.3. Behavioural discrimination under Art. 102(c) TFEU

An NCA would need to prove that the conditions of Art. 102(c) TFEU are given to sanction behavioural discrimination as an abuse of dominance. As discussed in section 3.2.1, discriminatory pricing is not *per se* a breach of Art. 102(c) TFEU. In particular, the NCA should prove that the dominant online platform has applied discriminatory pricing to "equivalent transactions" and that the discriminated customer has suffered a "competitive disadvantage" in comparison to "other trading partners". As argued in section 3.2.1, the recent *MEO* ruling has substantially increased the burden of proof for competition enforcers to sanction forms of behavioural discrimination under Art. 102(c) TFEU. In particular, the NCA has to consider "all the relevant circumstances" before concluding that the behavioural discrimination causes a competitive disadvantage for the discriminated customer.[236] For instance, the NCA should assess the bargaining power of the customer, the duration of the conduct and the presence of a discriminating strategy by the dominant online platform.[237] In order to satisfy the last criterion, the NCA should prove that the behavioural discrimination is a repeated conduct; a strategy systematically implemented by the online platform *vis-à-vis* certain customers. However, as discussed in the previous section, consumers/customers are often not aware of having been discriminated. Secondly, geographic discrimination could affect consumers based in different countries, outside of the NCA's jurisdiction. Finally, the NCA should analyse the functioning of the firm's algorithm to understand if the latter systematically discriminates different categories of consumers. The analysis of the algorithm would be a rather complex task for the NCA; the lengthy EU Commission investigations in the *Google Shopping* case are a good example to this regard.[238] In view of these considerations, the proof of the competitive disadvantage under the recent *MEO* case law would be a major challenge for any NCA committed to investigating behavioural discrimination under Art. 102(c) TFEU. In addition, it is worth noting that *MEO* has also

[236] *Supra,* Case C-525/16, para. 28.
[237] *Supra,* Case C-525/16, para. 31.
[238] The EU Commission opened investigations on Google in relation to the discriminatory of its search results in November 2010. After several attempts to negotiated commitments, which would require Google algorithm not to discriminate in terms of search results the products offered by the web site competing with Google Shopping service, the case was closed only in June 2017 via an infringement decision adopted by the EU Commission.
http://europa.eu/rapid/press-release_MEMO-17-1785_en.htm (22.5.2018).

introduced a presumption that exploitative price discrimination is unlikely to take place in practice.[239] The NCA would thus be required to rebut this presumption in order to sanction behavioural discrimination under Art. 102(c) TFEU.

Finally, the dominant online platform could in any case put forward a number of objective justifications.[240] For instance, the platform could argue that the behavioural discrimination leads to forms of optimal prices that increase the overall consumers' welfare. As argued above, price discrimination has a "mixed" effect on the consumers' welfare, and sometimes it can increase the welfare of "poorer" consumers. Therefore, the NCA should assess the impact of behavioural discrimination on the overall consumers' welfare of "budget conscious" and "affluent" consumers. On the other hand, the platform would have a hard time when it comes to justifying forms of behavioural discrimination among customers based in different EU Member States. In accordance with *United Brands* case law,[241] the Court of Justice has never accepted objective justifications *vis-à-vis* forms of price discrimination among customers based in different EU Member States.

To sum up, as argued in section 3.2.2, the existence of "alternative routes" does not obstacle the enforcement of Art. 102 TFEU *vis-à-vis* forms of behavioural discrimination by dominant online platforms. However, the NCAs would face a number of challenges in prosecuting such practice. First of all, as argued by the majority of economists and *de facto* recognized in CJEU case law, Art. 102 TFEU would be applicable only if the platform is super-dominant and the relevant market is characterized by high and persistent entry barriers; features that are rather unlikely in data markets. Secondly, the NCA would face a number of practical challenges when it comes to proving that the requirements of Art. 102(c) TFEU are given in accordance with the recent CJEU case law. In particular, in accordance with *MEO*, the NCA should collect evidence that behavioural discrimination is a repeated, rather than a sporadic conduct, and it would have to rebut the presumption that exploitative price discrimination is unlikely to be implemented by a dominant firm. Finally, the NCA should analyse the objective justifications put forward by the dominant online platform: with the exception of geographic behavioural discrimination, the NCA should conduct a case-by-case assessment of the impact of the contested practice on the overall consumers' welfare.

In view of these considerations, it is not surprising that no NCA has ever investigated any case of behavioural discrimination in data

[239] *Supra*, Case C-525/16, para. 35.
[240] *Supra*, Case T-301/04, para. 185.
[241] *Supra*, Case 27/6, para. 233.

markets. Similarly to excessive pricing, it is quite unlikely that any enforcement agency will explore this part of the *terra incognita* in the near future.

4.3. Unfair contractual terms in the data economy

So far, we have looked at theories of harm regarding excessive pricing and behavioural discrimination in the data economy. Here, lastly, we will have a look at unfair contractual terms imposed on final consumers by online platforms. As such, the analysis does not focus on "how much" users pay for online services in the form of personal data. Instead, the focus lies on the question whether the conditions imposed by dominant platforms are adequate and fair, or whether the conditions they make users consent to are too far reaching. Put differently, not the quantity of data collected is under scrutiny, but the question of how data are processed, who gets access, and how transparent the exchange of the deal "data against services" is. The critical link between consumers and dominant undertakings usually is the terms of service used by the latter. Insofar, as regards the theory of harm we are looking at here, there is a certain similarity to the discussion about "excessive pricing" in the data economy. Again, the question of whether or not exploitative conduct is given comes up because consumers oftentimes can use certain online services, such as web-messaging services or social networks, without providing a monetary payment. Instead, they "trade in" a bit of their privacy in the form of personal data. As such, the consent they give to the processing of their personal data at least partially serves as a payment.

We have already described above that the CJEU in its case law on Art. 102 TFEU has so far not provided a clear definition on when a contractual clause must be considered unfair. Even though the focus of the existing case law lies on industrial customers, there is no reason to *a priori* exclude unfair contractual terms imposed on final consumers from the scope of applicability of Art. 102 TFEU. Also, we assume in our analysis that users *de facto* do not have a choice what platform to use and must either use the services of the market dominant undertaking or abstain from using the services at all. As such, the terms of use are imposed unilaterally. The key question discussed here is under which circumstances terms and conditions imposed on consumers are an abuse of dominance under Art. 102 TFEU.

In this regard, two cases are worthy of further analysis, as they are topical and they cover different forms of conducts relevant from a competition perspective. Firstly, we will take a close look at the merger proceedings regarding Facebook and the messaging service WhatsApp (including its "aftermath"); secondly, we will analyse the

abuse of dominance proceedings by the German *Bundeskartellamt* against the social network Facebook.

4.3.1. The *Facebook-WhatsApp* merger and its aftermath

In 2014, the acquisition of WhatsApp by Facebook was cleared unconditionally by the European Commission and declared to be compatible with the internal market according to Art. 6(1)(b) of the EU Merger Regulation.[242] Without doubt, the amount of more than 20 Billion $ paid for a company with revenues of less than 20 Million $ could only be explained by the enormous long-term value of the consumer data Facebook gained access to through the transaction.[243] The European Commission saw no competition concerns regarding the three relevant markets affected by the transaction (i.e. consumer communication services, social networking services, and online advertising services).[244] As part of its competitive assessment, the EU Commission also discussed the possible integration of WhatsApp with Facebook, as was suggested by third parties. In particular, the EU Commission analysed the possibility that the companies could merge the personal data stored in both networks.[245] Facebook declared that for several reasons, "integration between WhatsApp and Facebook would pose significant technical difficulties".[246] The European Commission followed this statement, but declared that even if some degree of integration of users' databases was possible, it would not impact the result of the competitive assessment. This was the case in particular due to the "significant overlap between the networks" – i.e. the high number of users who already use both platforms anyway.[247] As such, the merging of data sets was eventually deemed not to be problematic from a competition law point of view.

When it comes to the corresponding implications for users' privacy, these were acknowledged by the EU Commission, but eventually also did not affect the outcome of the assessment. Instead, the Commission stated that any "privacy-related concerns flowing

[242] Council Regulation (EC) No 139/2004 (EC Merger Regulation);
Case No COMP/M.7217 – Facebook/Whatsapp, C(2014) 7239 final (hereinafter "Merger Decision"),
http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf (22.5.2018).
[243] Ceriello C. (2016), "EU Merger Regulation: A Protectionist Regime at Odds with U.S. Regulation?" 23 *Columbia Journal of European Law:* 477, p. 495.
[244] Cf. Recitals 142, 163, 190 of the Merger Decision.
[245] Recitals 136-140 of the Merger Decision.
[246] Recital 138 of the Merger Decision.
[247] Recital 140 of the Merger Decision.

from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules."[248] Considerations regarding consumer protection were not named during the assessment, neither from a factual nor from a legal point of view.

In August 2016, Facebook changed its "Terms of Service and Privacy Policy", since it had decided to indeed implement automated user-matching between Facebook and WhatsApp and, *inter alia*, did enable Facebook and its subsidiaries "to gain access to and use certain WA users' data, subject to a user control."[249] New WhatsApp users had to accept these conditions up-front; existing users had to choose in-app whether or not to accept data sharing between the two platforms within a 30-day period. Afterwards, their choice turned irrevocable.[250] In May 2017, the EU Commission imposed on Facebook/WhatsApp a fine of 110 Million € for negligently supplying incorrect and misleading information during the 2014 merger review proceedings.[251] The reason of the fine was that Facebook had not disclosed truthfully that already back at the time of the merger proceedings, it was technically possible to match the profiles of its users to those of WhatsApp in a manner that was at least sufficient for targeted advertising purposes. The "technical difficulties" Facebook relied on were of a significantly less severe nature than was claimed during the merger proceedings, and this was well-known to Facebook personnel. Yet, the EU Commission stressed again that even though the information provided by Facebook was incorrect (and the behaviour subject to a fine accordingly), this conduct did not have an impact on the competitive assessment of the merger, as was already stated in the merger decision.[252]

More interesting for our discussion are the proceedings by the Italian *Autorità Garante della Concorrenza e del Mercato* (AGCM). At roughly the same time of the EU Commission decision, the Italian Competition Authority imposed a fine of 3 Mio € on Facebook based not on competition concerns, but on an infringement of Italian consumer protection law.[253] The reason for the fine was, *inter alia*,

[248] Recital 164 of the Merger Decision.
[249] Case No. M.8228 – Facebook/WhatsApp, C(2017) 3192 final (hereinafter "Commission Decision on Fines"), Recital 45-46.
[250] *Supra*, Commission Decision on Fines, p. 10, footnote 18.
[251] The total fine comprises of a 55 Million € count each for supplying incorrect or misleading information a) in a notification made pursuant to Art. 4 of the Merger Regulation and b) in response to a request made pursuant to Art. 11(2) of the Merger Regulation, cf. Commission Decision on Fines, p. 24.
[252] Recital 100 of the Commission Decision on Fines.
[253] For the corresponding press release (in English), see http://www.agcm.it/en/newsroom/press-releases/2380-whatsapp-fined-for-3-million-euro-for-having-forced-its-users-to-share-their-personal-data-with-facebook.html

that Facebook "*de facto* forced the users of its service WhatsApp Messanger [sic] to accept in full the new Terms of Use, and specifically the provision to share their personal data with Facebook, by inducing them to believe that without granting such consent they would not have been able to use the service anymore." After the Terms of Use had been changed, users of WhatsApp were made to falsely believe that they had to consent to the passing on of their personal data to Facebook if they wanted to keep on using WhatsApp. According to the AGCM,

"this practice has been implemented through: a) an in-app procedure for obtaining the acceptance of the new Terms of Use characterized by an excessive emphasis placed on the need to subscribe to the new conditions within the following 30 days or lose the opportunity to use the service; b) an inadequate information on the possibility of denying consent to share with Facebook the personal data on WhatsApp account; c) the pre-selection of the option to share the data (opt-in); d) finally, the difficulty of effectively activating the opt-out option once the Terms of Use were accepted in full."[254]

Interestingly, the AGCM based its decision entirely on the Italian consumer protection law, rather than on competition or data protection law. During the proceedings, WhatsApp invoked the defence that its conduct was in compliance with data protection law, and thus could not be sanctioned as an infringement of the Italian Consumer Code. This defence was not accepted by the AGCM.[255]

Even though the Italian Competition Authority relied solely on consumer protection considerations, it might be argued that WhatsApp's conduct – i.e. urging users to consent to the data sharing between Facebook and WhatsApp by "tricking" them into agreeing even though the granting of consent was not necessary for further use of the service – could also be prosecuted as a unilateral imposition of unfair contractual terms under Art. 102 TFEU. In this regard, it does not play a role that WhatsApp's conduct was deemed to be in compliance with data protection law (at least this was the AGCM's view).[256] As we have already seen above in the *Astra Zeneca* case, "the illegality of abusive conduct under [Article 102 TFEU] is unrelated to its compliance or non-compliance with other legal rules and, in the majority of cases, abuses of dominant positions consist of

(22.5.2018) The competition authority also prosecuted WhatsApp because of some contractual clauses used *vis-à-vis* Italian consumers and deemed to be unfair, such as *"very wide and general exclusions and limitations of responsibility in favor of WhatsApp"* and the choice of law of the State of California in case of disputes.

[254] *Ibid.*

[255] Decision of the *Autorità Garante della Concorrenza e il Mercato* adopted on 11th May 2017 in the *WhatsApp Inc.* case, para. 36. The original text of the decision in Italian language is available at: www.agcm.it (22.5.2018).

[256] *Ibid.*, para. 50.

behaviour which is otherwise lawful under branches of law other than competition law."[257]

Also, the question whether WhatsApp's conduct was "unfair" and "unilaterally imposed" can be answered in the affirmative. By inducing users to consent to the data sharing with Facebook, WhatsApp asked for considerably more "remuneration" from its users (in the form of personal data) than was necessary for the provision of its services. The data fusion exceeded by far what consumers could have foreseen before the two companies merged, and considerably expanded the privacy implications, since the merging of the data sets potentially allows for the creation of highly detailed user profiles. Insofar, an analogy might be drawn to the CJEU case law in *BRT*.[258] According to this judgment, "all the relevant interests" [259] must be taken into consideration when assessing the contractual clauses. In *BRT*, the conduct of *SABAM* as a copyright collecting society was deemed a violation of Art. 102 TFEU because it imposed "on its members obligations which [were] not absolutely necessary for the attainment of its object and which thus encroach[ed] unfairly upon a member's freedom to exercise his copyright"[260]. Of course, WhatsApp is not a copyright collecting society, yet it also is a *de facto* unavoidable partner for many users who would like to use web-based messaging services, due to its market dominance. Ownership rights in personal (and non-personal) data do not exist. Still, the granting of consent to data processing under data protection law is comparable to granting a license, since it is equivalent to a form of commercialisation of one's data – at least in those situations when consent goes further than is necessary for the functioning of the service.[261] By making users believe that their consent is necessary to keep on using WhatsApp, the latter *de facto* imposed obligations that by far exceed what would have been necessary for the operation of the service. In consequence, the updated 2016 privacy policy is equivalent to a unilateral degradation of privacy to the detriment of the users.

The question remains open whether WhatsApp could invoke an objective justification for its demands, as is (at least in theory) possible according to *AAMS* case-law.[262] Nowadays, WhatsApp does

[257] Case C-457/10, AstraZeneca AB and AstraZeneca plc v. European Commission (2012) ECLI:EU:C:2012:770, para. 132.
[258] Case 127/73, Belgische Radio en Televisie and société belge des auteurs, compositeurs et éditeurs v SV SABAM and NV Fonior (1974) ECLI:EU:C:1974:25.
[259] *Ibid.*, para. 8.
[260] *Ibid.*, para. 15.
[261] *Supra*, Buchner and Kühling (2017), Art. 7, para. 11.
[262] As could be seen in Case T-139/98, Amministrazione Autonoma dei Monopoli di Stato (AAMS) v. European Commission (2001) ECLI:EU:T:2001:272, at least the EU General Court does not *a priori* exclude that dominant undertakings can invoke justifications for the unilateral imposition of unfair contractual terms.

not charge end users money for its services anymore.[263] Thus, WhatsApp might argue that as a "free" service (i.e. one that does not charge any monetary remuneration), its primary way to generate income is online personalized advertising. A prerequisite for the latter is access to personal data, which can be processed to generate user profiles for targeted advertising. Hence, WhatsApp could argue that getting users' consent to the processing of data stored on both networks is necessary for its business model to work in the first place, since the availability of more data allows for more and better targeted advertising. On the contrary, one could argue that even though access to personal data is indeed necessary for WhatsApp's business model, the merging of data stored on both networks is too far-reaching. Furthermore, even though the AGCM in this case found WhatsApp's conduct to be in line with data protection law, this finding is at least questionable: it is doubtful whether the consent given by users in this situation is really "freely given" and "informed",[264] since users were manipulated into agreeing to the new terms and conditions and were made to feel as if they did not really have a choice. As we have seen above, the legality of a conduct under a certain legal regime does not play a role for the question whether another legal regime is applicable or not. Yet, it is possible to take into account whether the rules and principles of another legal regime – in this case data protection law – have been followed or not when assessing the competitive impact of a certain conduct.[265] This means that privacy issues are not *per se* excluded from the competitive assessment, in particular when the processing of personal data is a significant element of the business model of an undertaking.[266] Hence, the method WhatsApp used to make users consent speaks further against an objective justification of its conduct. Depending on what line of argumentation one follows, it could easily be argued by an NCA that WhatsApp's conduct in this situation was a violation of Art. 102 TFEU.

4.3.2. The *Facebook* investigations by the *Bundeskartellamt*

Another closely related case is the abuse of dominance proceedings conducted by the German *Bundeskartellamt* against Facebook Inc. (USA), its Irish subsidiary and Facebook Germany GmbH (based in Hamburg).[267] In March 2016, the German Competition Authority formally initiated proceedings against Facebook based on the

[263] In several countries, such as Italy and Germany, WhatsApp used to charge an annual fee to end users. This is no longer the case.
[264] Cf. Art. 2(h) DPD, Art 4(11) GDPR.
[265] Cf. *supra*, Autorité de la concurrence and Bundeskartellamt (2016), p. 23.
[266] *Ibid.*, 23-24.
[267] Cf. the original press release (2 March 2016): www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html?nn=3591568 (22.5.2018),

suspicion that the social network abused its market power by violating data protection rules.[268] In December 2017, a more detailed preliminary assessment and background information to the proceedings were published by the authority. Based on the assumption that Facebook is a dominant company on the market for social networks in Germany, the *Bundeskartellamt* "holds the view that Facebook is abusing this dominant position by making the use of its social network conditional on its being allowed to limitlessly amass every kind of data generated by using third-party websites and merge it with the user's Facebook account."[269]

In the Statement of Objection published in December 2017, the *Bundeskartellamt* made a distinction between the collection and use of data on the network itself ("on Facebook"), and from third party websites ("off Facebook"). Only the latter is subject of the on-going investigation,[270] and refers to those websites and apps that have an embedded API with Facebook that allows for data sharing. This is not only the case for service providers owned by Facebook (e.g. WhatsApp and Instagram), but also for millions of other websites that, from a user's point of view, are not *prima facie* connected to the social network at all. All of these web sites and apps transfer personal data relating to users to Facebook, no matter if they, for instance, make use of Facebook's "Like Button" or otherwise actively engage in the data sharing.

Again, the terms of service (including its granting of consent to the processing of user data) are at the centre of the investigation and key to the competitive assessment. The *Bundeskartellamt's* accusations follow a two-step logic. Firstly, Facebook confronts its users with a "take it or leave it" offer. Users basically have to accept the excessive amount of Facebook's data collection, also from third party websites, without limits – or abstain from using the service at all. Secondly, the authority makes reference to infringements of the rules on data protection. The reference in the press release to the problematic "extent of data collection" can be seen as a hint at the "principle of data minimisation", which is probably violated by Facebook.[271] More explicitly with regard to consent, the competition

[268] The proceeding is based on German competition law, yet it can easily be analysed with a view to the European legal framework.

[269] See the authority's press release (19 December 2017), p. 1, www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2017/19_12_2017_Facebook.pdf?__blob=publicationFile&v=3 (22.5.2018, hereinafter "Press Release").

[270] This seems to be a means to streamline the investigation, since the authority *"leaves explicitly open whether [data collection and processing "on Facebook"] also constitutes a violation of data protection provisions and the abuse of a dominant position"* (Press Release, p. 2).

[271] Cf. Art. 6(1)(c) DPD, according to which personal data must not be "excessive in relation to the purposes for which they are collected". Also see the continuation of

authority states that "it can also not be assumed that users effectively consent to this form of data collection and processing."[272] As such, the violation of data protection law becomes a key part for the decision whether or not Facebook's conduct is abusive under Art. 102 TFEU. With a view to jurisdiction and competence, the *Bundeskartellamt* in its background paper (published together with the 2017 press release[273]) states that in those situations where access to personal data of users of a service is a significant factor for its market position, not only data protection authorities are responsible, but also the competition authority, when it comes to investigating how personal data are handled by the undertaking.[274]

It is not surprising that the *Bundeskartellamt* takes into consideration the legality of Facebook's conduct under data protection law as part of its competitive assessment, and thus makes it an integral part of its abuse of dominance investigations. In May 2016, the authority, together with the French *Autorité de la Concurrence*, expressed in a joint paper the opinion that even though data protection and competition law pursue different goals, the use of privacy policies and the corresponding processing of personal data can be taken into consideration if they affect competition.[275]

Time will tell how the *Bundeskartellamt* decides the case, or whether some kind of settlement with or commitment by Facebook will be reached. Lastly, it is noteworthy that in its publications regarding this case, the *Bundeskartellamt* makes reference to two of the privacy-related market failures described above.[276] The German NCA sees a "lack of transparency" with a view to Facebook's

---

this principle as given in Art. 5(1)(c) GDPR, which uses the stricter wording "limited to what is necessary in relation to the purposes for which [personal data] are processed".

[272] Press Release, p. 2.

[273] See the Background information provided by the *Bundeskartellamt* (19 December 2017), www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.pdf?__blob=publicationFile&v=6 (22.5.2018, hereinafter "Background Paper").

[274] Background Paper, p. 1-2.

[275] Cf. *supra*, Autorité de la concurrence and Bundeskartellamt (2016), p. 23-24: "Indeed, even if data protection and competition laws serve different goals, privacy issues cannot be excluded from consideration under competition law simply by virtue of their nature. Decisions taken by an undertaking regarding the collection and use of personal data can have, in parallel, implications on economic and competition dimensions. Therefore, privacy policies could be considered from a competition standpoint whenever these policies are liable to affect competition, notably when they are implemented by a dominant undertaking for which data serves as a main input of its products or services. In those cases, there may be a close link between the dominance of the company, its data collection processes and competition on the relevant markets, which could justify the consideration of privacy policies and regulations in competition proceedings."

[276] Cf. Section 3.1.

conduct, since the users' personal data are processed in a way they cannot expect.[277] This is even the case when users choose to disable "web tracking" in the settings of their browsers or take other active measures to protect their privacy.[278] Furthermore, it is claimed that Facebook makes users lose "control" over their personal data and that the privacy policy used should "provide them with suitable options to effectively limit this [extensive] collection of data."[279] This corresponds to the first market failure described above, since privacy preferences of many users cannot be catered for at the moment.

A last aspect that is worth discussing in relation to the *Facebook* case concerns the choice of the legal tool selected by the *Bundeskartellamt* to investigate Facebook's market behaviour, namely the equivalent of German competition law to Art. 102 TFEU. Colangelo and Maggiolino have recently criticized this choice, [280] arguing that the approach followed by the AGCM in the *Facebook-WhatsApp* case (i.e. relying on consumer, rather than competition law) seems more effective: the NCA should define the relevant market and prove the market dominance of the online platform – i.e. the NCA should satisfy a higher burden of proof to sanction unfair contractual clauses under competition, rather than consumer law. However, as recognized by Colangelo and Maggiolino themselves,[281] unfair commercial practices that affect consumers can be prosecuted in Germany either via litigation in civil courts or via mediation/arbitration. Unlike the Italian NCA, the German NCA currently does not have the power to adopt an administrative decision to sanction an unfair commercial practice under German consumer law. According to Colangelo and Maggiolino, the lack of a system of public enforcement of consumer law has led the *Bundeskartellamt* to investigate the *Facebook* case (i.e. a clear consumer law case) as an abuse of dominance case. In our view, the policy choice followed by the *Bundeskartellamt* should not be criticized. This choice confirms the argument put forward in section 3: competition, consumer and data protection law share a number of "family ties", but they pursue different objectives, have different scopes of application and different enforcement systems. When the NCA has a "choice" about the legal tool, it should have discretion in selecting the most appropriate "road". In particular, while it is true that a case pursued under consumer law implies a lower burden of proof for the NCA, since the authority is not required to assess the relevant market and the market power,

[277] Cf. Press Release, p. 2.
[278] Cf. Background Paper, p. 2.
[279] Press release, p. 2.
[280] Colangelo G., Maggiolino M. (2018), "Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook case for the EU and the U.S." *Transatlantic Technology Law Forum Working Paper No. 31*. The text of the working paper is available at: https://law.stanford.edu/publications/no-31-data-accumulation-privacy-antitrust-interface-insights-facebook-case-eu-u-s (22.5.2018).
[281] *Ibid.*, p. 25.

competition law offers more options in terms of remedies. As further discussed in section 5, under competition law the powers of the NCA are not limited to sanction the illegal conduct via the imposition of a fine. Instead, the NCA can conclude behavioural commitments with the dominant firm aiming at preventing a repetition of the infringement in the future.

4.3.3. Concluding thoughts

In this section we have analysed the *Facebook/WhatsApp* merger (including its aftermath, in particular the proceedings against WhatsApp by the Italian NCA based on consumer law considerations) and the abuse of dominance proceedings against *Facebook* currently conducted by the *Bundeskartellamt*. Especially with a view to the latter, the unilateral imposition of unfair contractual terms seems to be the most likely kind of exploitative conduct to be successfully prosecuted by an NCA in the near future. This type of exploitative conduct could either consist in a unilateral degradation of privacy standards for existing users (as was the case when Facebook integrated its platform with WhatsApp in order to match user profiles), or by simply using an abusive privacy policy in order to process personal data in an – for instance – excessive and non-transparent way, as is alleged by the *Bundeskartellamt* in the Facebook-investigation. The three areas of law discussed here – competition law, data protection law, and consumer law – seem to be seen in a more and more holistic manner by national authorities, which makes sense with a view to their shared "family ties" described in section 3.2.2. This might be seen as a first, small step towards a "closer dialogue" between these fields, as rightly promoted by the European Data Protection Supervisor.[282] Still, many more steps need to be taken by academics and NCAs alike in order to explore the remaining *terra incognita* in this field.

5. EU competition law remedies *vis-à-vis* exploitative conducts in the data economy

5.1. Fines – the right remedy?

As discussed in the previous section, in May 2017 the EU Commission imposed a fine of 110 million € on Facebook-WhatsApp for having provided misleading information during the 2014 merger review.[283] Fines are a traditional competition law remedy: the antitrust

[282] *Supra*, European Data Protection Supervisor preliminary opinion.
[283] *Supra*, EU Commission Decision on fines in *Facebook/WhatsApp*, p. 24.

enforcer sanctions *ex post* a market behaviour considered anti-competitive. Fines are usually coupled with a cease and desist order, whereby the NCA orders the parties to stop the contested behaviour.[284] Under EU competition law, different fines are available to sanction different types of conducts. In particular, the EU Commission can impose a fine of up to 10% of the worldwide turnover of the undertakings in order to sanction serious breaches of EU competition law (e.g. cartel or abuse of dominance).[285] Secondly, refusing to cooperate or providing wrong information to the EU Commission can lead to a fine of up to 1% of the firms' turnover.[286] As in the *Facebook-WhatsApp* case, the EU Commission can also impose a fine on the merging parties if the latter provide misleading information to the EU Commission during the process of the merger review.[287] Finally, daily payments can be imposed by the EU Commission if the undertaking either does not implement a Decision or does not comply with a binding commitment.[288] At the national level, fines are not harmonized.[289] However, NCAs "follow" the EU Commission's best practices when calculating antitrust fines on the basis of national competition law.[290]

---

[284] "Where the European Commission, acting on a complaint or on its own initiative, finds that there is an infringement of Article 101 or of Article 012 of the Treaty, it may by decision require the undertakings and associations of undertakings concerned to bring such infringement to an end…".
Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L-1/1, 4.1.2003, Art. 7(1).

[285] *Ibid.*, Art. 23(2).

[286] *Ibid.*, Art. 23(1).

[287] Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation), OJ L-24/1, 29.1.2004, Art. 14(1).

[288] Art. 24(1) Reg. 1/2003.

[289] At the national level, NCAs calculate the applicable fine for an infringement of Art. 101-102 TFEU on the basis of the parameters provided under national competition law. In March 2017, the EU Commission published a legislative proposal to harmonize the enforcement powers of NCAs. In particular, the draft Directive harmonizes the fines imposed by NCAs for breaches of Art. 101-102 TFEU: similarly to the EU Commission, the NCAs will be able to impose a fine up to 10% of the worldwide turnover of the undertaking, as well as daily payments. The Directive is currently pending for approval by the Council and the European Parliament.
European Commission, Proposal for a Directive of the European Parliament and the Council to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market (ECN+ Directive), Brussels, 22.3.2017, COM (2017) 142 final, Art. 13-15.

[290] In particular, in calculating the gravity of the infringement and possible attenuating circumstances, several NCAs follow the criteria mentioned by the EU Commission in its 2006 guidelines on fines calculation. In relation to the convergence of antitrust fines calculation, see Dunne N. (2016), "Convergence in Competition Fining Practices in the EU" 53 *Common Market Law Review*: 453-492.
EU Commission, Guidelines on the method of setting fines imposed pursuant to Article 23(2)(a) of Regulation No 1/2003, OJ C-210/2, 1.9.2006.

The cumulative fines imposed by the EU Commission and by the Italian NCA in the *Facebook-WhatsApp* case well represent the limits of this antitrust remedy in the context of the data economy. Although the two authorities imposed independent sanctions related to violations of different legal regimes (i.e. EU Merger Control Regulation and Italian Consumer Law), the fines originated from (roughly) the same behaviour – i.e. the integration of WhatsApp's user database into Facebook and the way the companies communicated their plans and actions towards their users and the authorities. The antitrust theories of harm in the context of the data economy are still *terra incognita;* an area that academics and enforcers currently have only started to explore. Since the legality of a market behaviour under EU competition law is not always straightforward, firms face difficulties in understanding what types of conduct are compatible with EU competition law in the context of the data economy. Secondly, a fine coupled with a cease and desist order will seldom manage to effectively "turn the clock back" to the pre-infringement scenario. For example, in January 2018 the Italian NCA imposed a second fine on Facebook-WhatsApp for not having implemented the previous decision of May 2017.[291] The latter decision required the merging parties to publish an extract of the AGCM's decision on WhatsApp's web site, in order to inform WhatsApp users of the misleading nature of the Terms of Use accepted in 2014. However, the concentration has already been implemented and the users' databases have already been integrated. Therefore, even if the consumers were informed of the misleading nature of WhatsApp's Terms of Use, the decision of the Italian NCA would not be able to restore the consumers' choice.

Similar arguments can be put forward in relation to the administrative fines that other enforcers could impose on online platforms. In particular, the GDPR has significantly increased the maximum fine that the data protection authorities can impose for a violation of data protection law. The national supervisory authorities can now impose a fine of up to 4 % of the total worldwide annual turnover (of the preceding financial year) of the undertaking in order to sanction serious breaches of privacy law, such as the processing of personal data without the user's consent or the illegal transfer of personal data to third countries.[292] Following the entry into force of the GDPR in May 2018, the fines imposed for breaches of data protection law are thus expected to increase in the majority of the EU Member States. However, an open question is whether and to what extent the increased fines will be sufficient to deter violations of privacy law by online platforms.

[291] Decision of the *Autorità Garante della Concorrenza e il Mercato* adopted on 10 January 2018 in the *WhatsApp Inc.* case. The original text of the decision (in Italian language) is available at: www.agcm.it (22.5.2018).
[292] Art. 83(5) GDPR.

5.2. Behavioural commitments in the data economy

As argued in the previous section, due to the new challenges posed by competition law enforcement in the data economy, NCAs should "guide" firms' behaviour, rather than sanction it. Under Art. 9 Reg.1/2003, the EU Commission can conclude commitments with the undertakings subject to a competition law investigation under Art. 101-102 TFEU. Commitments are also common in the field of merger control, where they represent a valid alternative to a prohibition decision.[293] Finally, at the national level most of the NCAs have the power to negotiate commitments in the context of competition law investigations, even though the extent of this power varies from country to country.[294]

Commitments are, generally speaking, divided into "structural" and "behavioural" remedies.[295] The first category includes commitments that aim at solving the anti-competitive behaviour via a "divestiture" of the firm's assets (such as shares in another firm, business units, patents…), whereby the firm's market power within the relevant market is reduced. On the other hand, behavioural commitments are an open category of remedies that can be jointly designed by the firm and the NCA. Via a behavioural remedy, a firm commits to behave in a certain manner in the future, in order to "prevent" a competition law violation (for instance, the firm might agree to continue the supply of a competitor for a certain period of time). Behavioural commitments work *ex ante*, and thus they are placed at the borderline with market regulation.[296]

At the EU level, both structural and behavioural commitments follow similar steps from a procedural point of view: at any time during the investigations, the firm(s) concerned may approach DG Competition, declaring its/their willingness to settle the case.[297] The EU Commission will consider the possibility to settle the case only if

[293] "The European Commission may attach to its decision under paragraph 1(b) conditions and obligations intended to ensure that the undertakings concerned comply with the commitments they have entered into *vis-à-vis* the Commission with a view to rendering the concentration compatible with the common market."
Art. 6(2) Reg. 139/2004.

[294] Under the draft ECN+ Directive, all NCAs will have the power to accept commitments from undertakings involved in investigations concerning a breach of Art. 101-102 TFEU.
Art. 11 draft ECN+ Directive.

[295] For a detailed analysis of the EU Commission practice in relation to commitments adopted under Art. 9 Reg. 1/2003, see Dunne N. (2014), "Commitment Decisions in EU Competition Law" 10(2) *Journal of Competition Law and Economics:* 399-444.

[296] *Ibid.*, p. 411.

[297] European Commission, Notice on best practices for the conduct of proceedings concerning Articles 101 and 102 TFEU, OJ C-308/6, 20.10.2011, para. 118.

the alleged infringement does not require the imposition of a fine.[298] The proposed commitments have to be accepted by the EU Commission and are later subject to a "market test", in order to verify the competitors' reactions to the proposed remedies.[299] Finally, the EU Commission will adopt a formal decision, making binding the agreed commitments for the undertaking(s).[300] As mentioned above, the breach of such a decision could lead the EU Commission to impose a fine on the undertaking(s).[301] Finally, both structural and behavioural commitments will be monitored by a "trustee": an independent expert appointed by the EU Commission, who will supervise the process of divestiture of the assets concerned and/or check periodically the compliance with the behavioural remedies by the undertaking concerned.[302]

Since the enactment of Reg. 1/2003, commitments have become a common antitrust remedy, especially in cases involving breaches of Art. 102 TFEU.[303] Commitments create a number of advantages both for the undertakings and the antitrust enforcers. On the one hand, by accepting a commitment, the undertaking reduces the risk of follow-on damage actions and does not harm its reputation.[304] In addition, the undertaking can offer solutions "tailor-made" to its needs. On the other hand, by accepting commitments rather than adopting an infringement decision, the EU Commission can speed up the

[298] Recital 13 Reg. 1/2003.
[299] *Supra*, Commission Notice on best practices in Art. 101-102, para. 129.
[300] Art. 9(1) Reg. 1/2003.
[301] Art. 24(1)(c) Reg. 1/2003.
[302] *Supra*, Commission Notice on best practices in Art. 101-102, para. 128.
[303] An updated list of the commitment decisions adopted by the EU Commission since the entry into force of Reg. 1/2003 is available on the DG Competition web site.
http://ec.europa.eu/competition/elojade/isef/index.cfm?clear=1&policy_area_id=1 (22.5.2018).
[304] Under *Masterfoods* case law, national courts "cannot adopt decisions running counter to that of the Commission" under Art. 101-102 TFEU. Therefore, if the EU Commission sanctions a cartel agreement, the Decision will be a proof of infringement of EU competition rules that will bind a national civil court in the context of a follow-on damage action. The latter tribunal will only have to quantify the damage suffered by the plaintiff and establish a causal link with the infringement sanctioned by the EU Commission. The Damages Directive has extended the binding value of the NCAs decisions on national civil courts as well. Nevertheless, commitment decisions do not represent a proof of infringement of EU competition rules. In such a case, the civil court will have to ascertain whether an infringement of EU competition rules has taken place; the commitment decision will not bind the civil court.
Case C-344/98, *Masterfoods Ltd v. HB Ice Cream Ltd.* (2000) ECLI:EU:C:2000:689, para. 52.

Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union, OJ L-349/1, 5.12.2014, Art. 9.

investigation process, and it can avoid the risk of losing the case on appeal at the GC/CJEU.[305] In spite of their advantages, commitments have been criticized in the literature due to the lack of legal certainty about the legality of a market conduct, and for by-passing judicial control.[306] Furthermore, the EU Commission has been criticized for the large use of commitments in network industries (e.g. energy); industries where commitments have been relied on by the EU Executive to achieve liberalization objectives that were not politically feasible under the sector specific EU Directives.[307] Finally, commitment negotiations are not always as "speedy" as expected, especially when competitors are reluctant to accept the proposed commitments in the context of the market test: the lengthy and unsuccessful negotiations between Google and DG Competition in the context of the *Google Shopping* case are a good example to this regard.[308]

As recognized by a 2016 House of Lords' report, the length of commitment negotiations is a possible obstacle to the enforcement of this type of antitrust remedy in the context of the digital economy.[309] Besides the reluctance of competitors to give "green light" to the proposed commitments, the length of the negotiations may also be caused by the technical complexity of the remedies proposed.[310] On the other hand, the report also recognizes that commitments are

[305] Since the commitments are offered by the undertaking, it is very unlikely that the undertaking may have any incentive to later appeal the EU Commission Decision under Art. 263 TFEU.

[306] To this regard, see for instance Monti G. (2008), "Managing the intersection of utilities regulation and EC competition law" 4 *Competition Law Review:* 121.

[307] In relation to the antitrust commitments concluded by the EU Commission with a number of energy operators in order to this liberalize this industry, see:
- De Hautecloque A., *Market Building through Antitrust* (Edward Elgar Publisher, Cheltenham 2013).
- Sadowska M. (2011), *Energy Liberalization in Antitrust Straitjacket: a Plant too Far?* 34(3) *World Competition:* 449-476.

[308] The EU Commission opened investigations in the *Google Shopping* case in November 2010. In April 2013, Google proposed a number of commitments, aiming at solving the competition concerns expressed by DG Competition. In particular, Google would have modified the functioning of its search algorithm, in order not to discriminate web sites competing with Google Shopping. After several years of negotiations, the EU Commission rejected the proposed commitments and adopted an infringement Decision in June 2017.
The chronological steps of the Google Shopping case are available at:
http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39740 (22.5.2018).

[309] UK House of Lords, Select Committee on European Union, "Online Platforms and the Digital Single Market", 10th Report of Session 2015-16, published on 20th April 2016, para. 188. The text of the report is available at:
https://publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/129.pdf (22.5.2018).

[310] *Ibid.*, para. 191.

flexible in terms of design.[311] In particular, since they are "tailor-made", commitments better fit the peculiarities of the data economy in comparison to prescriptive regulation.[312] While structural commitments are generally excluded in the context of the data economy, since they would affect direct network externalities and thus the consumers' welfare,[313] behavioural commitments are considered a possible alternative to fines and cease and desist orders; an alternative that would allow the NCA "to guide" the industry players and to fill in the gaps in the regulatory framework.

According to Bary and De Bure, the main limit of behavioural commitments in the context of the data economy concerns their duration.[314] Due to reasons of legal certainty, the EU Commission/NCA usually accepts commitments that bind the firm(s) for a fixed period of time. Commitments usually last for a number of years; a period in which the business freedom of the firm(s) subject to the commitments is substantially restricted. The EU Commission/NCAs usually include a review clause in the commitments decisions. Nevertheless, according to the authors, these clauses are rarely enforced in practice, unless new and unforeseeable circumstances take place in the market.[315] According to Bary and De Bure, behavioural commitments are "rigid" and they do not match the peculiarities of modern digital markets, characterized by disruptive innovation and sudden changes of the market structure. A competition issue that requires a behavioural remedy today might be outdated in few years' time, due to the entry of a new competitor in the market that can quickly acquire market power due to the release of an innovative product. The authors, therefore, propose the introduction of active review clauses in commitment decisions affecting digital markets. Such clauses could be structured in different manners. First of all, remedies could be "conditional" – i.e. they could be applicable

[311] "… we note that the flexible, principle-based framework of competition law, which can be customized to individual cases, is uniquely well-suited to dealing with the subtlety, complexity and variety of possible abuses that may rise in these markets. We cannot see how a less flexible regulatory approach could be more effective."
Ibid., para. 187.
[312] *Ibid.*, para. 187.
[313] In 2014, the European Parliament proposed to "un-bundle" Google as a possible remedy to solve the *Google Shopping* case. However, the EU Commission did not take up the proposal. Similarly to the divestiture of datasets, in fact, such radical remedy might negatively affect the ability of the firm to innovate and thus harm the consumers' welfare.
European Parliament, Resolution on Supporting Consumer Rights in the Digital Single Market, Strasbourg, 27.11.2014, 2014/2973(RSP), para. 15. The Resolution is available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2014-0071+0+DOC+XML+V0//EN (22.5.2018).
[314] Bary L., De Bure F. (2017), "Disruptive Innovation and Merger Remedies: How to Predict the Unpredictable?" 3 *Concurrences:* 1-9.
[315] *Ibid.*, p. 5.

only if certain conditions take place in the market within a certain period of time.[316] Alternatively, the NCA could include in the commitment decision either an "automatic" review clause (e.g. commitments are abolished if there is a new entrant in the market), or a "periodical" review clause carried out by the monitoring trustee.[317] The latter would assess periodically the structure of the market, and thus would re-examine whether and to what extent commitments are still needed. Bary and De Bure discuss the issue of flexibility of behavioural commitments in relation to mergers involving firms operating in digital markets. However, their conclusions could also be applicable to commitments decisions concluded under Art. 9 Reg. 1/2003.

In the next two sections, we explore the use of behavioural commitments to tackle discriminatory/excessive pricing and unfair contractual clauses as described in section 4.

5.3. Behavioural commitments *vis-à-vis* excessive and discriminatory pricing in the data economy

In this paper we have argued that EU competition law can in principle sanction excessive and discriminatory pricing in the context of the data economy. However, as recognized in section 3.2.1, this type of enforcement of Art. 102 TFEU should only take place in rather "exceptional circumstances" – i.e. in relation to super-dominant online platforms and in markets characterized by high and persistent entry barriers. In addition, in section 4.2 we have provided empirical evidence about the presence of behavioural discrimination in the data economy: the use of algorithms and big data allows online platforms, to some extent, to discriminate their customers by charging the maximum retention price that the individual customer would be willing to pay for a certain product or service.

While there are good reasons to advocate the enforcement of Art. 102 TFEU to sanction excessive and discriminatory pricing in the context of the data economy, we have also argued in sections 4.1 and 4.2 that NCAs and the EU Commission would face several challenges in satisfying the standards elaborated by the CJEU case law to sanction these types of exploitative conducts under Art. 102. For instance, in a digital world characterized by "free" services,[318] it would be rather difficult to apply the traditional *United Brands*

[316] *Ibid.*, p. 7.
[317] *Ibid.*, p. 8.
[318] In the paper, we have argued that online "free" services actually have a "price" in terms of personal data provided by the user to the platform in exchange of the service.

cost/price test to show the presence of excessive pricing.[319] Similarly, comparing the "price" of an online "free" service with the "price" of a similar service provided by competing platforms in accordance with *Latvian Copyright Society* would be a rather complex task for an NCA.[320] Also, it would be hard for a competition authority to show that a discriminated customer has suffered a "competitive disadvantage" and to rebut the presumption that exploitative price discrimination is unlikely to take place in practice; a presumption recently introduced by the CJEU in *MEO*.[321] In addition, both in the case of excessive and discriminatory pricing, the NCA should show that the anti-competitive conduct is a repeated, rather than a sporadic conduct, and that it has a negative impact on consumers' welfare. Finally, the NCA should assess the arguments put forward by the dominant platform to justify its behaviour.

Due to these challenges it is thus unlikely that any NCA will explore this area of the *terra incognita* in the near future. Nevertheless, if an NCA was "brave enough" to follow this un-explored route and found enough convincing evidence to sanction an online platform due to excessive pricing/behavioural discrimination under Art. 102 TFEU, the issue of defining suitable remedies would suddenly "pop up". A fine coupled with a cease and desist order would probably be an unwise solution, due to the lack of precedents in this area. Yet, by working in cooperation with the dominant firm, the NCA could design a number of behavioural commitments which aim at solving the contested practice. In particular, we argue that 3 types of remedies could tackle issues related to excessive/discriminatory pricing imposed by dominant online platforms:

> 1) Price comparison web site: a dominant online platform would be able to discriminate its customers and charge the maximum retention price only if the customers did not have "any other choice" – i.e. the platform was an un-avoidable trading partner. This could be the case if the platform was the only provider of a certain type of product or service – i.e. a scenario quite unlikely in the modern Internet era, where we can order products from every corner of the world. On the other hand, the customers would also be locked-in in case they were not aware of any other better offer for the same type of product offered by the platform. The Internet provides countless offers, but users are often not aware of them. They usually buy products from the most well-known online platforms, such as Amazon, eBay etc. Trust is an essential component of internet sales. A new online platform often faces challenges when it comes to winning the consumers' trust as regards the reliability of its services. Thus,

[319] *Supra*, Case 27/6.
[320] *Supra*, Case C-177/16.
[321] *Supra*, Case C-525/16.

trust represents an important entry barrier in digital markets; a barrier that encourages consumers to buy services from the incumbent platforms, which in turn reinforces their dominant position. Trust is a barrier for a new entrant in the "real" economy, too. However, due to the "long-distance" nature of digital transactions, trust is an entry barrier in the digital world: a consumer is unlikely to buy any product/service or to use a new platform before having read positive feedback from other previous users.

Price comparison web sites encourage internet users to compare offers provided by different platforms, by thus reducing the barriers that new entrants face in the digital world in terms of "trust". Price comparison web sites have become a rather common tool to compare products that are mostly purchased online, such as hotel and flights bookings,[322] while they are less common in other markets characterized by a limited number of providers of a certain product. For instance, while price comparison web sites for airline tickets are rather common, this type of web site is less common and less relied on by consumers for other means of ground transportation. In the case of trains, for instance, only few firms operate the same line; price comparison web sites are thus less common in this sector, and users are thus required by themselves to make search queries on the web sites of the different providers.

An NCA/the EU Commission could consider the introduction of a price comparison web site as a potential behavioural remedy to solve issues of excessive and discriminatory pricing by super-dominant platforms. The latter would be a suitable remedy in industries where a price comparison web site does not exist yet, and thus the market does not offer this type of services to consumers (i.e. market failure). In regulated industries, a number of National Regulatory Authorities (NRAs) operate their own price comparison web sites to allow consumers to compare offers. This encourages consumers to check and (maybe) switch their suppliers, and this in turn fosters the degree of competition in the newly liberalized markets.[323] At the conclusion of its

[322] In Europe, Booking.com is the main price comparison web site specialized in hotel bookings. On the other hand, a number of web sites such as SkyScanner, Kayak and Expedia are specialized in comparing airline tickets. In both cases, hotels and airlines pay a small commission to these web sites when a consumer books hotel/flight via these web sites. The latter, therefore, do not directly provide any service, but they rather act as intermediaries between the final consumers and the service providers.

[323] For instance, the Austrian Energy Regulatory Authority (E-Control) has established a web site to compare the electricity and gas tariffs offered by different suppliers in Austria. The web site works like a price comparison web site, automatically generating queries on the web sites of the different energy providers

investigations, showing the presence of excessive and discriminatory pricing by a dominant online platform, the NCA could establish its own price comparison tool, relevant for the industry subject to investigations. An NCA could not be accused of regulating the market; it would rather increase the degree of transparency of the industry for final consumers. Secondly, in case this type of remedy was introduced in regulated markets, the NCA could actively cooperate with the relevant NRA to provide the service. Finally, the remedy would not be "permanent": as soon as the market offered a similar price comparison service and there were signs that consumers switched to alternative providers, the NCA could stop providing the service.

2) Limiting the number of data collected by the platform: online platforms can discriminate their customers due to the large number of personal data they collect. Even in the presence of anonymized data, via data fusion and data analytics the platform can infer the individual retention price and use this information to discriminate its customers. As further discussed in the next pages, an NCA/the EU Commission could impose a number of limitations on the types of data gathered by the platform. Such a remedy could borrow concepts from the relevant data protection legislation. However, when needed, it could go even further: it could solve the market failures described above, such as the lack of transparency of data protection terms and the recurring lack of effective data anonymization. As discussed in section 3.1, data protection law is oftentimes not suitable to solve these issues in modern digital markets, since, for example, it still mostly relies on the concept of consent. Via its behavioural remedy, the NCA/EU Commission could overcome the issue of lack of informed users' consent, by indicating what types of personal data the platform would be allowed to collect, for how long, and for which purposes. This type of remedy would clearly have a "regulatory" character, and it would overlap with the relevant data protection regime. As discussed in section 3.2.2, data protection law does not hinder in principle the enforcement of EU competition law. Secondly, this type of regulatory intervention by the NCA/EU Commission would be justified only in the presence of an abuse of dominance by a super-dominant platform in the form of excessive and discriminatory pricing – i.e. a rather exceptional scenario. Finally, when

on the basis of the consumers search inputs. The service is provided free of charge by E-Control and can be found here: https://www.e-control.at/en/konsumenten/service-und-beratung/toolbox/tarifkalkulator (22.5.2018).

designing the applicable remedy, the NCA could actively cooperate with the competent data protection authority in order to identify "gaps" in the data protection regime which could be filled via the NCA's behavioural remedy.

3) Sharing the customers' data with competing platforms: as mentioned above, online platforms can discriminate their customers due to the large amount of data they collect from their customers and the ability to build user profiles via data analytics. Instead of asking the platform to reduce the amount of data collected and thus hampering possible efficiencies generated by data analytics, the behavioural remedy could require the online platform to "share" a number of its customers' data with competing platforms. This type of remedy has also been applied by the European Commission in the airline industry: a number of concentrations, in fact, have been cleared by the EU Commission subject to the condition that the merging parties open their frequent flyer programs to competing airlines.[324] Travellers can now redeem and acquire miles by traveling with competing airlines. This encourages flyers to switch to other operators. However, by making compatible the frequent flyers' programs of the merging parties and their competitors, the EU Commission *de facto* required the merging parties to share important data about their frequent flyers (i.e. the premium customers) with competitors. The latter could then target the frequent flyers with ad-hoc offers.

This type of remedy could also be taken into account in digital markets, by requiring the super-dominant online platform to share some information about its customers with its competitors. As a result, competitors would be able to target the customers of the dominant firm with ad-hoc offers, and consumers would thus be encouraged to switch suppliers.

As noted by Colangelo and Maggiolino, a data sharing remedy would pose a number of enforcement problems for the NCA. First of all, it would be hard for the NCA to define from the outset which data would be subject to the duty to share.[325] As mentioned in the previous pages, the ability to extract useful information via data analytics rather than the amount of cumulated data grants market power to a dominant platform.

[324] This type of remedy was imposed by the EU Commission in the following merger decisions:
- Commission decision of 14.10.2010. Case COMP/39.596, *BA/AA/IB.*
- Commission decision of 23.5.2013. Case COMP/AT.39595, *Continental/United/Lufthansa/Air Canada.*
- Commission decision of 12.5.2015. Case COMP/AT.39964, *Air France/KLM/ Alitalia/Delta.*

[325] *Supra*, Colangelo /Maggiolino (2017), p. 274.

> Therefore, data sharing might not be sufficient to re-balance the competitive disadvantage suffered by the competitor of the dominant firm if the latter does not have access to the technology/algorithms to process the data shared. Secondly, data (sometimes) have a limited lifespan, depending on the context. Thus, sharing obligations might prove to be useless for the competitor of the dominant firm after a certain amount of time has passed.[326] Finally, it would be hard for the NCA to define *a priori* the price for the sharing of data.[327] The value of a dataset is rather subjective, and it is strongly influenced by the possible outcomes of data analytics. These challenges show the need for the EU Commission/NCA to conclude commitments with the parties, rather than imposing unilaterally a behavioural remedy. By making use of commitments, remedies can be designed that match the needs of the dominant firm and the new entrants. Secondly, as discussed in section 5.3, a review clause should be included in the behavioural decision in order to adjust the remedy to changing market conditions (if necessary).

So far, these types of remedies have never been applied by any NCA. It remains to be seen when and whether any competition enforcer will be "brave enough" to sanction a dominant platform under Art. 102 TFEU due to excessive and discriminatory pricing. However, in such a case, these types of remedies would probably be more suitable to solve the anti-competitive conduct at stake, rather than a fine coupled with a cease and desist order.

5.4. Behavioural commitments vis-à-vis unfair contractual clauses in the data economy

5.4.1. Data protection and behavioural commitments – an oxymoron?

In section 3.1, we have analysed three market failures that arise in the data economy in the context of the processing of personal data. Two of these market failures primarily result from the so called "privacy paradox". We have found, firstly, that oftentimes the market does not cater for the expressed privacy preferences of users, since consumers are confronted with a "take it or leave it" lock-up situation. The market does not provide what users actually demand, while at the same time consumers "give in" and do not abstain from using those services that do not fulfil their privacy needs. Secondly, we have discovered a recurring "lack of transparency": in many online situations, privacy policies are so comprehensive, illegible and vague

[326] *Supra*, Colangelo/Maggiolino (2017), p. 275.
[327] *Supra*, Colangelo /Maggiolino (2017), p. 275.

that lay people cannot realistically fully understand the terms and conditions. Instead, consumers simply "consent" without making a truly informed decision. As such, the factual situation does not live up to the idea behind the concept of informational self-determination, even though the rules on data protection might be formally complied with.

In the following pages, we will show that these two market failures might be solved – or at least mitigated – by behavioural commitments that take recourse to the rules and general principles contained in the General Data Protection Regulation. We argue that, in this context, behavioural commitments based on the GDPR's provisions might serve as adequate remedies. Furthermore, by way of example, we will apply the same approach to one kind of market failure which is outside of the rather specific scope of the two privacy-centred market failures discussed above: we will look at social networks and the data portability provision given in Art. 20 GDPR. Social networks are multi-sided platforms, and as such naturally belong to a kind of market with a tendency to produce market failures. The difference to the market failures we have described before lies in their origin. For social networks, the problem is not only the "privacy paradox" and the resulting imbalance between the respective interests of the users and the provider/advertisers, but network effects that lead to market concentration. Still, we argue that entering into a behavioural commitment that is based on the before mentioned data portability provision might also serve as an adequate remedy in this situation.

The approach presented here may seem unorthodox at first, since the primary goals of competition and data protection law are different in nature. Compliance with data protection law is obligatory for all undertakings, no matter if they are market dominant or not. As such, the imposition of rules that are applicable anyway would not provide for added value. Furthermore, as we have already discussed above in a more general context, one might argue that data protection infringements should be prosecuted by data protection authorities and not by means of behavioural commitments under EU competition law. Yet, for various reasons, implementing data protection rules via behavioural commitments might be a reasonable and efficient tool to foster competition in some situations.

The idea behind our proposal is that the rules given under data protection law primarily aim at safeguarding privacy and other fundamental rights. As such, they might serve as a valuable starting point when it comes to solving an existing imbalance "between privacy and disclosure",[328] which has tipped to the detriment of data

[328] *Supra*, Acquisti (2012), p. 227. For the definition of market failure used in this text, see above section 3.1.2.

subjects. The behavioural commitments discussed here could serve as a tool to change this balance in favour of users as far as this is necessary from a competition policy perspective. Furthermore, and on a more general level, our approach might generally be feasible when data protection rules also serve competition policy goals, as we will see with a view to the example of social networks and the data subjects' right to data portability given in Art. 20 GDPR.

5.4.2. Increase of legal certainty

A commitment by a market dominant undertaking might help to clarify cases of doubt as regards the lawfulness of a particular conduct. Being an *omnibus legislation* applicable in a variety of entirely different situations,[329] the GDPR contains a couple of rather open provisions that are subject to interpretation, such as the "principles relating to processing of personal data" given in its Article 5, or the scope of the "right to data portability" as given in its Article 20. Another example for newly-arisen legal uncertainty would be the "right to be forgotten" as granted in Art. 17 GDPR, which needs to be interpreted and substantiated further both by the courts and academia.[330] As such, insecurity prevails in many situations as regards the legality of specific conducts, especially in those fields where the GDPR introduced significant changes of law. Hence, a commitment between the EU Commission (or an NCA) and a market dominant undertaking can result in legal certainty for the latter, as regards both compliance with competition and data protection law. This might serve as a strong incentive for cooperation, in particular with a view to the (severe) administrative fines that can now be imposed under the GDPR.[331] From this point of view, it might also be feasible to include the competent data protection authority in the process of negotiating a commitment in order to streamline the negotiations and ensure full compliance with both legal regimes. This idea is also embraced by the *Bundeskartellamt*, which is cooperating

[329] On this term and on the difference between the EU's "omnibus" approach to privacy legislation as opposed to the sector-by-sector approach taken by the United States, see Schwartz P. M. (2013), "The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures" 126(7) *Harvard Law Review:* 1966, p. 1973-1975.

[330] Cf. Di Ciommo F. (2017), "Privacy in Europe after Regulation (EU) No 2016/679: What Will Remain of the Right to Be Forgotten?" 3(2) *The Italian Law Journal:* 623, p. 628-629.

[331] Under the GDPR, *"administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher"* can be imposed for infringements (of most) of the provisions contained in the Regulation: Art. 83(5) GDPR. It has been heavily criticized in the literature that infringements of clauses as vague and open to interpretation as Art. 5(1) GDPR are subject to these heavy fines, cf. *supra*, Gola in Gola (2017), Art. 83, para. 19.

with the data protection authorities in its on-going Facebook investigations described above.[332]

5.4.3. Use of behavioural commitments as "safety net" based on existing provisions

Secondly, as part of behavioural commitments, obligations that reach further than the rules given under the GDPR can be imposed on undertakings and thus serve as tailor-made answers to existing market failures. One might apply a provision contained in the GDPR and, using this mandatory minimum threshold as a basis for the behavioural commitment, extend its scope of applicability. As a result, market dominant undertakings are subject to stronger obligations than smaller ones, yet the obligations remain similar in nature. This flexible and contextual approach might be helpful in those situations where there is a market failure (in the form of an inadequate balancing of privacy and commercial interests), because the regulatory minimum provided under the GDPR does not suffice to uphold effective competition. Competition law enforcement in the form of behavioural commitments would act as a "safety net" in those cases where data protection regulation – which naturally aims at protecting privacy instead of competition – does not lead to satisfactory results.

5.4.4. Markets do not cater for users' privacy preferences

We have found that oftentimes markets do not cater for the actual privacy preferences users have, and this eventually leads to bigger privacy losses than users would actually be willing to accept if they had a choice. Getting back to the Facebook investigations by the *Bundeskartellamt* described above, the authority in its press release finds that "consumers must be given more control over [data collection from third party websites] and Facebook needs to provide them with suitable options to effectively limit this collection of data."[333] This (preliminary) finding points directly to the alleged abuse of dominance: users do not have a choice which social network to use. At the same time, they have to accept the privacy policy in full when setting up an account and are restricted to the privacy options presented to them by Facebook when using the network. Here, an appropriate balance between the users' privacy interests and Facebook's commercial interests is *de facto* not reached.

[332] Cf. *supra*, Bundeskartellamt Background Paper, p. 2: "*In its assessment of whether the company's terms and conditions on data processing are unfair, the competition authority does, however, take account of the legal principles of data protection laws. For this purpose, the Bundeskartellamt works closely with data protection authorities.*"

[333] *Supra*, Bundeskartellamt Press Release, p. 2.

There are several conceivable solutions to this problem, all of which are "inspired" by the role consent plays in the GDPR,[334] and could easily be integrated into a behavioural commitment. For instance, the social network could commit to offering more detailed privacy settings to its users, which allows them to "fine tune" their privacy settings. This could be more or less granular: one might give users the option to decide what kinds of personal data Facebook is allowed to collect from third party websites. Alternatively, one might give users a choice which third party websites shall be allowed to transfer data to Facebook, or whether they would prefer to block data access entirely. Hence, if being tracked is no problem for a user and he/she prefers personalized advertising over neutral ads, they can allow Facebook to collect the data. If they do not feel at ease with this kind of data collection, they can choose not to allow the data transfers but, for instance, pay a monthly fee to Facebook instead.[335]

Many more options are conceivable and of course the behavioural commitment would need to be well-designed and based on a thorough assessment of all relevant aspects, such as the specific market conditions, observed users' behaviour etc. Still, the overall idea of tackling the market failure with recourse to the consent principle given under the GDPR and the underlying right to informational self-determination seems promising, and fair, for all parties involved.

5.4.5. Lack of transparency

We have also found that a recurring problem of online business models is a lack of transparency: users oftentimes consent to online privacy policies without actually properly reading and fully understanding them. The reason behind this situation is that on the one hand, users do not really care, while on the other hand, they are simply not able to meaningfully grasp and comprehend these terms and conditions. Again, the validity of the consent given is the Achilles' heel, and again, the pending *Facebook* case serves as a good example to analyse.

When it comes to making terms on consent when drafting a behavioural commitment, there is a certain degree of leeway as regards "how" data subjects should be requested to give consent. In some situations, it might be desirable to make users well aware of what exactly they consent to, and to "force" them to decide deliberately. Insofar, the system has already changed in favour of users, as the GDPR has abolished the "opt-out"-system: under the

[334] Cf. Art. 4(11), 6(1)(a) and 7 GDPR.
[335] As regards these considerations see above, section 3.1.5.

GDPR, users always have to actively "opt-in". This means that, for instance, a pre-ticked box cannot constitute valid consent anymore.[336] Also, the controller must now be able to demonstrate that consent was given when it serves as the legal basis for the processing of personal data (*i.e.* the burden of proof now lies with the data controller, Art. 7(1) GDPR).[337]

Yet, as part of a behavioural commitment, one could go further than that if deemed necessary. For instance, when a data controller wants to engage in data processing that goes significantly further than what a regular user would legitimately expect, the introduction of a so called "double opt-in" could be required as behavioural commitment (i.e. a two-step confirmation that consent is granted). "Double opt-in" in this context could mean that users have to actively change their privacy preferences (step 1), and then they have to confirm the new settings by clicking on a link that has been sent via e-mail (step 2). This would still allow Facebook and other social networks to pursue their business model, and at the same time safeguard the users' right to informational self-determination. Generally speaking, one could demand different levels of explicitness of the consent given based on the respective context. Alternatively, one could make consent "expire" after a certain period of time. For instance, it might make sense to ask users to confirm their consent again after expiry of a 6-month period. This would raise their awareness of what is currently happening to "their" personal data and would mitigate the lethargy that regularly results from the "privacy paradox".

5.4.6. Social networks and data portability

Lastly, we will have a closer look at one kind of market failure that does not result from the "privacy paradox" and is not directly connected to the issue of the validity of user consent. Social networks are prone to market concentration due to network effects, and thus might be critical from a competition law point of view.[338]

Social networks, such as other data controllers, are subject to Art. 20 GDPR, which grants data subjects a "right to data portability". This means that under certain circumstances, data subjects have the right

[336] Cf. Recital 32 GDPR: *„Silence, pre-ticked boxes or inactivity should not (…) constitute consent. "*

[337] Cf. *supra*, Buchner/Kühling in Kühling/Buchner (2017), Art. 7, para. 57-58.

[338] Graef I. (2015), "Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union" 39(6) *Telecommunications Policy:* 502, p. 503-504.

"to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided"

In addition, under Art. 20(1) and (2) GDPR, data subjects the right to demand that "personal data are transmitted directly from one controller to another, where technically feasible". This bundle of rights (i.e. the right to data portability) has two dimensions: a data protection dimension, as it serves to "further strengthen the [data subject's] control over his or her own data",[339] and a competition policy dimension, as it aims at reducing lock-in effects and switching costs for users and thus stimulates competition by making it easier for users to switch to competitors.[340] The right to data portability only refers to personal data which have been "provided" to the controller by the data subject. As such, non-personal data (i.e. those that have been rendered anonymous and those that are anonymous *per se*) are excluded from its scope of applicability from the outset. Furthermore, all personal data referring to a data subject that have been uploaded to the social network by other users are excluded as well.[341]

In many situations, the right to data portability might not be problematic or controversial at all, such as when it comes to the transfer of personal data stored "in the cloud" to another cloud service provider. Yet, the right to data portability is particularly cumbersome in the context of social networks – even though they had been on the mind of the lawmaker, since social networks had been named explicitly as a use case for data portability in the Commission's original 2012 draft of the GDPR.[342] In the context of social networks, in fact, data portability is difficult to implement for several reasons. For instance, technical burdens must be overcome due to the very different software "architecture" of social networks and their internal logic and functionality.[343] Also, those parts of a social network which qualify as personal data – such as a picture of the data subject – but have not been uploaded by the respective data subject themselves would not be included in the data portability claim that data subjects have, since they have not been "provided" by them (as stipulated in

[339] Recital 68 GDPR.
[340] *Supra,* Graef (2015), p. 507-508; Piltz C. in Gola (*supra,* 2017), Art. 20, para. 1-3.
[341] *Supra,* Graef (2015), p. 507.
[342] Cf. the Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Recital 55: *„The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one."*
[343] Cf. *supra,* Graef (2015), p. 507.

Art. 20(1) GDPR) but by someone else. Yet, those personal data uploaded by someone else might still be considered to be an integral part of a person's profile. Looking at it from another angle, the latter aspect also has a legal dimension, as third party rights, such as those of other users of the social network (stemming from data protection and intellectual property law) must also be cleared before the porting of data to another social network can take place.[344] In practice, these factors might *de facto* uphold the lock-in effects social networks have, and as such mitigate both the positive data protection and competition effects originally envisaged by the drafters of the GDPR.

In such an unsatisfactory situation, entering into a behavioural commitment with the social network provider based on the underlying rationale of Art. 20 GDPR might make sense. For instance, as part of such a commitment, one could think of extending the scope of applicability of Art. 20 GDPR to non-personal (*e.g.* anonymized) data or include third party data as far as necessary to meaningfully port profiles. This would make data portability more meaningful and effective when a social network is market dominant. Of course, when it comes to porting data belonging to third parties, a solution would have to be found to ensure compliance with, for instance, their data protection and IP rights. A method would need to be implemented to ensure, for instance, that a legal basis for the processing of the personal data of third parties is given up-front, such as consent according to Art. 6(1)(a) GDPR, and that no copyrights are violated. In addition to modifying the data portability requirements given under the GDPR, one might also consider the fostering of interoperability between social networks. Yet, as regards the latter, a regulatory approach might be more effective, as only general interoperability requirements could ensure that also new, small social networks partake from the outset.[345]

5.4.7. Concluding thoughts

In this section, we have argued that behavioural commitments between market dominant undertakings and competition authorities should, in some situations, be drafted based on the rules and principles contained in the GDPR. This might serve to adequately remedy an unwanted imbalance between the privacy interests of users and the commercial interests that undertakings have in data disclosure. Our approach is particularly well-suited when it comes to those market failures that stem from the so called "privacy paradox", such as the "lack of transparency" problem we have described above. Furthermore, our approach might also be useful when it comes to

[344] *Ibid.*
[345] *Ibid.*, p. 510.

other kinds of market failures that have a particular relevance from both a data protection and a competition law point of view. By way of example, we have analysed the situation of social networks and how a behavioural commitment could be designed based on the right to data portability as given in Art. 20 GDPR.

We are aware that our approach is unconventional, and that some issues would need to be addressed and analysed further. A general problem – as is always the case with behavioural commitments – is that commitments barely ever undergo judicial review and, as such, might foster a certain degree of legal uncertainty on an abstract level. Yet, from the point of view of the undertakings concerned, entering into such a commitment holds the promise of individual legal certainty, as they do not run the risk of being found in violation of competition or data protection provisions. This is even more attractive with a view to the newly established, severely high administrative fines that can be imposed under the GDPR in case of data protection infringements (cf. Art. 83(5) GDPR). Furthermore, especially when close cooperation to data protection authorities is sought during the process of negotiating the commitments, this might actually even contribute to legal certainty for other undertakings as well. In data protection matters, it is quite common to retrieve informal advice from data protection authorities up front in case of uncertainty as regards the legality of specific conducts, as it is a field of law that regularly requires a significant amount of balancing of interests. As such, behavioural commitments might even provide general guidance on how to interpret the GDPR's provisions.

In sum, our approach might serve to inspire tailor-made and contextual remedies in a field that is still developing and which consists, to a large extent, of *terra incognita* for undertakings, authorities, and the lawmaker alike. The cautious combination of competition law and data protection law that we have argued for might be a fruitful opportunity to appreciate the "family ties" that these legal regimes have in common.

6. Conclusions – the results of the preliminary exploration of the *terra incognita*

This paper represents our first attempt to explore the enforcement of EU competition policy in the data economy (i.e. the contemporary *terra incognita).* The data economy generates a number of opportunities to improve the production and marketing of existing products, as well as to provide new services to consumers. The data economy thus generates a number of new business opportunities that have the potential to increase the consumers' welfare. However, it also

poses new questions and challenges as regards the enforcement of EU competition law.

In our journey we have followed the "shortest route" towards the East India: rather than circumnavigating Africa as other authors have done before (i.e. by analysing issues connected to the relevant market and market power definition in the digital economy), we directly sailed towards the West, by looking at enforcement challenges and potential remedies under EU competition law. In particular, we have discussed the role that EU competition law could have in sanctioning exploitative conducts by dominant online platforms under Art. 102 TFEU, such as the imposition of excessive and discriminatory pricing, as well as the use of unfair contractual clauses. Therefore, we have travelled in a *terra* truly *incognita*, which has not been previously covered in the literature.

In our journey we have relied on the limited number of "maps" available, mainly consisting of the CJEU case law on exploitative abuses (in section 2). Afterwards, we have discussed possible market failures in the data economy (in section 3.1), as well as potential arguments against the enforcement of EU competition law *vis-à-vis* exploitative conducts. In particular, we have assessed the economists' sceptical views on EU competition law enforcement *vis-à-vis* excessive and discriminatory pricing in view of the relevant CJEU case law (in section 3.2.1). Secondly, we have discussed the overlap between competition, data protection and consumer law in this area (in section 3.2.2). Our conclusion is that data economy is characterized by a number of market failures; failures that indeed call for competition law intervention. In particular, in spite of their "family ties", competition, data protection and consumer law do not replace each other. However, EU competition law should intervene only in rather "exceptional circumstances"; in particular, EU competition policy should sanction discriminatory and excessive pricing only in the presence of super-dominant firms and high entry barriers.

Although the enforcement of EU competition law *vis-à-vis* exploitative conducts in data markets should be exceptional, but not impossible, the NCAs/EU Commission would face a number of challenges in applying the relevant CJEU legal standards to sanction these types of abuses under Art. 102 TFEU. As argued in section 4.1 and 4.2, the EU Commission/NCAs would have a hard time when it comes to sanctioning excessive and discriminatory pricing by dominant online platforms in accordance with the standards recently defined by the CJEU in *Latvian Copyright Society* and *MEO*. Therefore, although possible in theory, the enforcement of Art. 102 TFEU *vis-à-vis* excessive and discriminatory pricing in the data economy seems unlikely in the near future. By contrast, it would be easier for an NCA or the EU Commission to satisfy the CJEU legal standards to sanction unfair contractual clauses by dominant online

platforms under Art. 102 TFEU (cf. section 4.3). The recent *Facebook/WhatsApp* merger case and the on-going *Facebook* investigations in Germany are examples of an emerging trend in this regard.

We have completed our journey in the *terra incognita* in section 5, by discussing possible remedies that the NCA/EU Commission could take into consideration to sanction exploitative conducts by dominant online platforms. We have argued that due to the lack of precedents in this area, fines coupled with cease and desist orders do not seem to be the most appropriate remedy. By contrast, the competition enforcer should guide the market players via behavioural remedies; tailor-made commitments agreed with the dominant firm. In section 5.3 we have speculated on possible remedies in cases concerning excessive and discriminatory pricing in the digital economy, such as the introduction of a price comparison web site, as well as the obligation imposed on the dominant platform to either reduce the number of collected customers' data or to share some information with competitors. By contrast, in section 5.4 we have argued that in designing the behavioural remedies in relation to unfair contractual clauses imposed by dominant online platforms, the NCA/EU Commission should look at the relevant data protection legislation. In particular, the behavioural commitments could either clarify the unclear aspects of the GDPR or extend the scope of its obligations and application. In designing the applicable remedies, the NCA/EU Commission will have to actively cooperate with the relevant authorities, such as the competent data protection authority.

Due to the limited number of court rulings and NCA decisions in this area, these conclusions are preliminary, and rather speculative. This paper represents a first attempt to explore the *terra incognita*. Other sailors will further continue this journey and contribute to the lively debate that issues linked to the data economy are expected to produce in the coming years.