eLaw
Working Paper Series

No 2019/004 - ELAW– 12 April 2019_Rev. 30 September 2019

Big data analytics contracts in the EU: A nexus between digital platforms' regulation & private law?

Serge J.H. Gijrath

Universiteit Leiden
eLaw

Big data analytics contracts in the EU: A nexus between digital platforms' regulation & private law?

Prof. dr. Serge J.H. Gijrath, eLaw@Leiden University[1]

ABSTRACT

This Article reflects on big data analytics agreements in light of the EU Commission's desire to safeguard a fair, innovation-friendly business environment for and effective competition on digital platforms.[2] Following an introduction of big data and relevant artifcial intelligence (AI) notions, the Article considers whether the use of online tracking methods for big data analytical purposes conflicts between the EU digital platforms' data regulation favoring the free flow of non-personal data and the private user rights in terms of data transfer agreements (DTAs) to which they are not a party. This Article is not concerned with personal data regulation. Rather it asks several related questions, such as: to what extent can contracts function as a lever when pseudonymized and/or anonymized non-personal data are transferred by a controller to a third party unknown to the private user. Should stakeholders have access to the terms in big data transfer agreements (DTAs)? At the core of this Article lies the question whether and how private indviduals should be enabled to contest big data analytics exercises. A supplementary question is whether consumer law van be a powerful tool for private users against he controller who sells and transfers these non-personal data to a third party. In terms of DTA's for big data analytics purposes, the discussion is rekindled whether (big) data may qualify as property under the law. The final remarks reconcile the different policy & legal goals.

Key Words: Big Data Analytics Contracts; Consumer Protection; Data Ownership, Data Protection; Data Subjects; EU Digital Platforms Regulation, GDPR, Legal Qualification of Big Data; Nexus of contracts; Private Law; Private Users.

---

[1] Endowed professor of telecommunications and ICT law, elaw@Leiden, and attorney-at-law/partner, C-Legal, Amsterdam, the Netherlands. The author advises clients in the IT, media and electronic communications sector. He has no direct or indirect links to either the European Commission, Facebook or Cambridge Analytica. This article is based on independent research and reflects the objective findings and personal opinions of the author. A draft version of this Paper was published within the eLaw Working Paper Series at Universiteit Leiden, No. 2019/003 ELAW, 12 April 2019. Article closed on 9 May 2019.
[2] Article closed 30 September 2019. The author wishes to thank is colleague Karolina La Fors, post-doc researcher at Leiden University, for her insightful comments. This Article extends the presentation at Universitat de València, "Reconciling Big Data Analytics Contracts with Digital Platforms' Regulation" to include private law notions; keynote speech, *Competition Law, Digital Platforms and Big Data, Conference Paper*, 2018.

1. Introduction: Big Data, you are beautiful…

1.1 Context, research questions & structure

> "*Big data is no fad. (…) [T]he application of big data analytics has spread throughout the public and private sectors. Almost every day I read news articles about its capabilities and the effects it is having, and will have, on our lives. My home appliances are starting to talk to me, artificially intelligent computers are beating professional board-game players and machine learning algorithms are diagnosing diseases*."[3]

The scope and depth of big data analysis is likely to have a tremendous impact on the daily lives of private individuals, without them always being aware of that. How can they contest big data output that affects them? This Article looks at the possible nexus between data transfer agreements (DTAs) and general terms and conditions (GTC).

The first part of this Article sets the stage: the main themes are the data economy, digital platforms' regulation, the role of platform providers and data protection regulation.[4] A brief discussion of the different approaches to the data economy is presented in para. 1.2. Facebook's privacy policies from 2018 revealed what a digital platform provider expects to do with private user data gathered at the platform's entrance gate. When data are in the hands of a third party whose business is aimed at selling big data analytics reports, the tracking of how data have been assembled, processed and analysed is near impossible. Para. 2 discusses whether online tracking methods create a dichotomy between digital platforms' regulation and DTAs.

The second part of this Article discusses the autopoiesis between private and big data law. It explores the notion of transparency in general terms and conditions as an effective tool for redress, when third parties do not perform big data analytics properly.[5] Para. 3 reflects high-level on legal qualifications of data ownership (including personal information) given by legal scholars. The common thread in this Article is private user/consumer empowerment against unwanted re-use, transmission and/or

---

[3] Information Commissioner's Office, UK, *Big data, artificial intelligence, machine learning and data protection,* Report, v. 2.2, 20170904, 2017 (ICO 2017). Some definitions (big data; AI) were found in the footnotes of this report; reference is made to the original source and this writer's access thereto.

[4] In this Article, the providers of digital platform access and services will be labelled broadly as 'platform providers', also when they fall under the definition of online intermediaries. See Regulation (EU) 2019/115 of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, *OJ L 186, 11.7.2019, p. 57–79,* (the Online Intermediary Services Regulation). See also Council Position, Press Release, of 29 November 2018.

[5] Online Intermediary Services Regulation, 4th para. This Article is not focused primarily on analysing the various competition law administrative actions against social media platforms.

processing of pseudonymized[6] and/or anonymized data. Theories of property law, intellectual property law, freedom of information or currency notions are discussed briefly. It will also be considered whether and how big data contracts fit into private law, in particular contract law. Returning to the concerns that surfaced in the context of the Cambridge Analytica (CA) case, para. 4 offers some thoughts on how the processing big data for analytics purposes could (and should) be regulated by applying private law notions.

The research for this Article is aimed at seeing to what extent data protection law and private law could be aligned. This Article contends that private law can supplement data protection law in a meaningful way, when a *nexus* is created between big data protection and consumer law.[7]

1.2 A little history of big data

Big data analytics is often referred to as a combination of big data, AI and machine learning.[8] The proposal on the free flow of non-personal data applies a broad notion of data processing. It includes data analytics services, which is the focus of this Article.[9] An often used definition of big data is:

> *"[H]igh-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making."*[10]

---

[6] See Article 4 (5) GDPR: (5) "'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"; see also: M. Mourby, E. Mackey, M. Elliot et al., "Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK", *Computer Law and Security Review*, Volume 34, Issue 2, April 2018, Pages 222-233.

[7] See, e.g., N. Helberger, F. Zuiderveen Borgesius and A. Reyna, "The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law", *Common Market Law Review* 54: 1427-1466, Kluwer Law International, 2017 (Helberger, Zuiderveen Borgesius, Reyna, 2017). The contribution predated the Cambridge Analytica incident and new regulation such as the Online Intermediary Services Regulation.

[8] Academics from different backgrounds use the term AI in one breath with 'machine learning'. In short, machine learning is a technical process that underpins and facilitates the use and output of AI. See also: "The Outlook for Big Data and Artificial Intelligence (AI)", *IDG Research*, 11 November 2016, https://idgresearch.com/the-outlook-for-big-data-and-artificial-intelligence-ai/ Accessed 6 September 2019.

[9] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal data in the European Union, OJ L 303/59, 28 November 2018, entry into force May 2019 (Free Flow of Non-Personal Data Regulation).

[10] *Big data refers to the exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large*

The characteristics of big data are determined often by the possibilities that the volume thereof brings for analytical and statistical purposes. High-velocity is required to process the gargantuan data volume and the variety of data to determine trends. Veracity of big data analytics is driven by the use of AI and machine learning.[11] Yet, AI is not intended for a linear analysis of data in the manner they have been processed or programmed. In general, AI consists of the analysis of data to model some behavioural aspects. Inferences from these models are used to predict and anticipate possible future events.[12] The added value of applying AI is the learning capacity.[13] AI may create intelligent responses to new data and adapt output accordingly. The ability to analyse data is considered valuable for society as a whole, because it could lead to "better" and more informed decision making."[14] In big data analytics, personal data are no longer prevalent (although they may be). *Prima facie*, that could entail that personal data issues are not a big concern for private users any longer. After all, the transfer concerns raw or stripped data, and what is wrong with that? Without really being aware of it, the user characteristics morph depending on how the platform providers process

organisations, which are then extensively analysed (hence the name: analytics) using computer algorithms"; Article 29 Working Party (WP29) – now the European Data Protection Board (EDPB): *Opinion 3/2013* on purpose limitation. See also the data policy discussed in part 1 below. See on the policy: WP29 Statement on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, 16 September 2014 (*WP 221*). Other relevant documents include: WP29 Opinion 03/2013 on Purpose limitation, WP 203; WP29 Opinion 06/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217; WP Opinion 05/2014 on Anonymisation Techniques, WP216. See also: Council of Europe. *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 01/2017.The latter part "decision making", currently is inciting most of the legal academic debate. See also: Gartner IT glossary Big data. http://www.gartner.com/it-glossary/big-data; accessed on 21 March 2018.

[11] J. Modrall, "Big Data and Algorithms, focusing the discussion", Oxford University, *Business Law Blog*, 15.1.2018 (Modrall 2018).

[12] UK Government Office for Science, *Artificial intelligence: opportunities and implications for the future of decision making,* 9 November 2016 (ICO 2016).

[13] A recent OECD study qualified as a major risk of the use of algorithms that their application could assist the data analytics companies or their clients to sustain profits above the competitive level more easily without necessarily having to enter into an agreement; OECD, *Algorithms and Collusion – Background Note by the Secretariat*, DAF/COMP, (2017) 4 (OECD 2017), p. 24. At the same time, OECD signalled that it was difficult to draw conclusions on the technological question whether algorithmic interaction can be considered as to be a "meeting of the minds" under the definition of agreement covered by competition rules, OECD 2017, p. 36-37 (OECD 2017).

[14] European Data Protection Supervisor, "Meeting the challenges for big data, a call for transparency, user control, data protection by design and accountability", *Opinion 7/2015*, EDPS 19 November 2015 (EDSP 2015).

and transfer data. Besides being (1) data subjects within the meaning of the GDPR,[15] the subscribers to digital platforms and online intermediary services are: (2) end-users of the content/services on such platforms, and (3) consumers.[16]

Marketing companies have collected and processed data of groups of consumers forever. Yet, as will be seen below, there may be a false resolve here. Input for big data analytics often is collected directly and endlessly by the service provider from online customers or on the digital (social media) platforms they use. Batches of data are transferred to third parties. The delineation between personal and non-personal data blurs. It seems that third partied consider aggregated non-personal data to be outlawed and that anything goes. Is the use of non-personal data harmless?[17] The analytics process enables the processor to mine data for new insights and to find correlations between apparently disparate datasets. Serious concerns arise when big data analytics output is used also for harmful purposes. This Article argues that big data analytics do not necessarily result in *better informed* decision making.[18] If the data analytics process is not managed well, this could lead to harmful consequences for private users. A case in point is discussed briefly in sub-paragraph 1.4.

1.3 Digital platforms, big data and competition

Big data must be seen through the Commission's desire to promote the free movement of data, as part of enhancing the internal market's data economy. The Commission earmarked the data economy as a key objective in its Digital Single

[15] See the General Data Protection Regulation, Council Regulation (EU) 2016/679 of 27 April 2016, *OJ L* 119/1, 4 May 2016 (GDPR).

[16] Hence, they are referred to often in this Article as 'private users.' Clearly and arguably, there is interaction between (small) businesses on digital platforms as well; professional companies are less likely to benefit from a consumer law approach; but they do need to understand that they should contract for data use and sharing. See also: L. Determann, "No One Owns Data", *Hastings Law Journal*, vol. 70:1, 2019 (Determann 2019).

[17] See also the data policy discussed in part 1 below. See on the policy: WP29 Statement on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, 16 September 2014 (*WP 221*). Other relevant documents include: WP29 Opinion 03/2013 on Purpose limitation, WP 203; WP29 Opinion 06/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217; WP Opinion 05/2014 on Anonymisation Techniques, WP216. See also: Council of Europe. *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 01/2017.

[18] "*Big data refers to the exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed (hence the name: analytics) using computer algorithms*"; Article 29 Working Party (WP29) now the European Data Protection Board (EDPB): *Opinion 3/2013* on purpose limitation.

Market (DSM) strategy.[19] Applications such as Internet of Things (IoT),[20] Machine to Machine (M2M) communications and Blockchain and its Trust Protocol are examples of how data analysis is going to affect daily life. Big data analytics' possibilities really amount to the take-off and landing of everything. Data mining is the tool. Rather than looking at the downsides – which were left to GDPR discussions, the Commission formulated concrete policy objectives that could be translated into regulation in order to achieve the internal market objective of a European data economy,[21] while creating a level playing field and a secure environment for big data analytics. The starting point was the stimulation of the potential of data for business, research and innovation purposes.[22] The Commission focused its policy on: (1) securing free flow of data within the Union;[23] (2) providing for data access and transfer;[24] (3) liability issues[25] and (4) data portability. [26] Under the internal market this should perhaps also entail a harmonized approach to enabling consumers to monitor how harmful big data analytics may be contested. But there is no direct link to regulating consumer protection against big data as of yet.[27] The Commission has also focused on the competition aspects of digitization. As part of its Digital Single Market (DSM) strategy, the Commission

[19] https://ec.europa.eu/commission/priorities/digital-single-market_en; Commission Communication "Building A European Data Economy" (Commission Communication 2017); see also: Commission Communication "On the Mid-Term Review on the Implementation of the Digital Single Market Strategy – A Connected Digital Single Market for All", {SWD(2017) 155 final}, COM (2017) 228 (Commission Communication DSM 2017).

[20] WP29 Opinion 08/2014 on Recent Developments on the Internet of Things, WP223.

[21] Commission Communication, "Building a European data economy", COM(2017) 9 final. Consultations ongoing. See also Commission Staff Working Document, accompanying the document Communication Building a European data economy {COM(2017) 9 final}, SWD (2017) 2.

[22] M. Granieri, A. Renda, *Innovation Law and Policy in the European Union, Towards Horizon 2020*, Springer, 2012 (M. Granieri, A. Renda, 2012).

[23] Free Flow of Non-Personal Data Regulation.

[24] Mostly the GDPR; although, arguably some of the digital platforms regulation contains comparable provisions, i.e., Regulation 2017/1128/EU of the European Parliament and of the Council of 14 June 2017 on Cross-border Portability of Online Content Services in the Internal Market, [2017] OJ L 168/1 including corrigendum to regulation 2017/1128; Regulation 2018/302/EU of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) no 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC, [2018] OJ L 601/1; and fairly specific (and out of scope of this article), the languishing Directive 98/84/EC of the European Parliament and the Council of 20 November 1998 on legal protection of services based on, or consisting of, conditional access, [1998] OJ L 320/54.

[25] Under construction with different legal approaches competing, i.e., liability under the GDPR or contractual and extra-contractual liability; see below.

[26] This is part of the GDPR, see, e.g., articles 13 and 20.

[27] The Digital Content Directive takes a consumer protection approach; see The Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services ("*Digital Content Directive*").

launched a competition sector inquiry into e-commerce in May 2015 to identify possible competition concerns arising from companies' online business practices.[28] An important finding was that, where data analytics companies utilize algorithms to process big data, this could result in restrictive agreements, decisions or concerted practices under article 101 TFEU. Yet, these practices may be difficult to contest, especially where the company imposes very one-sided data agreements on its customers. As can be inferred from EU investigations against digital platforms, valuable big data that are not replicable may create anti-competitive market power for the party who controls the either the input data and/or the big data collection. But, in light of the free movement of non-personal data, the Commission's view may be two-sided. The Commission has expressed concerns about inability to access digital services. Conversely, it fears innovation could be stifled if the access threshold is too high.[29] The possible competition concerns relate to data-collection and usage.[30] This could create competition concerns where the same players are in direct competition for the sale of certain products or services.[31] Hence, the focus is on remedies and fines, rather than on empowering consumers.[32] An important question should be whether a consumer should be informed in a more transparent way prior to automated decision making (ADM) resulting from big data analytics.

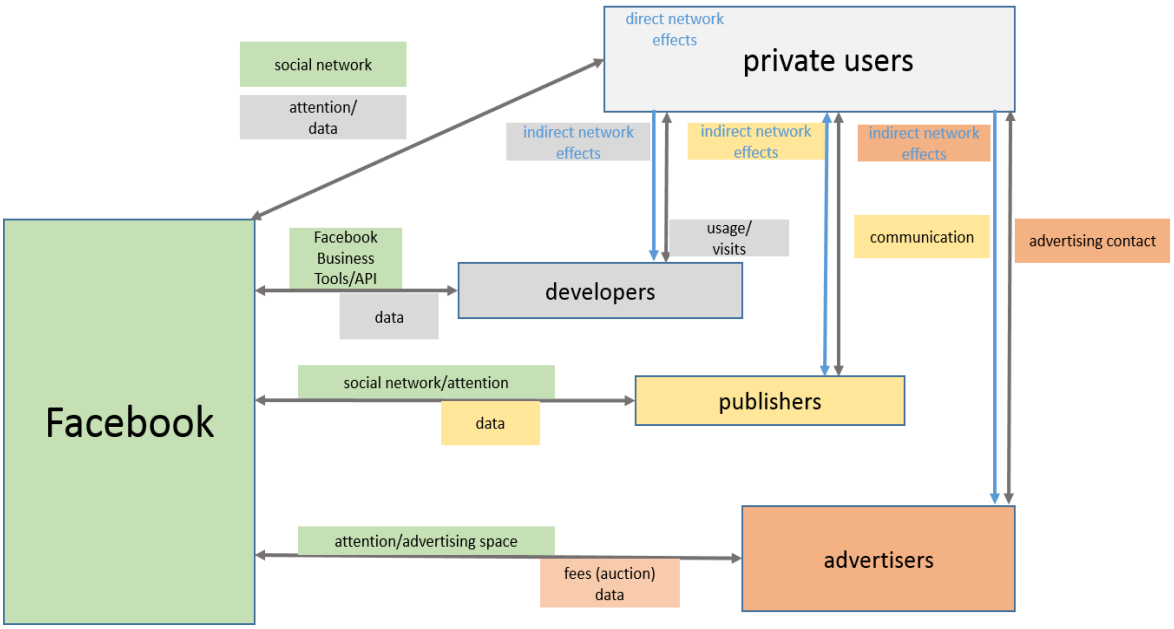
1.4 Case in point: when big data analytics go horribly wrong

In 2018, the (ab-)use of data by big data analytics' companies indeed proved to be a worrisome case of aggregated personal data being transferred third parties.[33] In 2019, the German Federal Cartel Office ('FCO', *Bundeskartellamt*) – following an investigation of Facebook into abuse of a dominant position – handed down a final

[28] Commission, Final report on the E-commerce Sector Inquiry {SWD (2017) 154 final} COM(2017) 229 (Sector Inquiry 2017).
[29] Market Parties are asking for intervention. See, *i.e*., G. Soros, "Only the EU can break Facebook and Google's dominance", *The Guardian*, 15 February 2018.
[30] Two examples: Commission Decision approval of the merger and subsequent fines in *Facebook/WhatsApp,* M.7217, 29.08.2014 and its decision in *Google Search Shopping,* Case AT.39740, 27.06.2017. The Commission imposed a hefty fine of € 2.42 billion to *Google* for abusing its market dominance as a search engine by giving an illegal advantage to another Google service, notably its comparison of shopping services.
[31] Sector Inquiry 2017, p. 14.
[32] *Infra*, para. 1.4.
[33] By the end of 2018 the UK's ICO had imposed a fine of UKL 500.000 on Facebook.

ruling in first instance.[34] The FCO established that Facebook was limitlessly – and often without purpose – amassing *every kind of data* on its private users.[35] The FCO investigation relates to the way digital platforms with embedded APIs, in this case Facebook, its subsidiaries, including WhatsApp and Instagram, shared the personal data of their private users.[36] The FCO's ruling contains an impressive legal novelty. The novelty is that the consumers are not seen solely as data subjects. The FCO looks at consumer protection of private users, too. The FCO establishes a dominant position of Facebook. It goes further in that it considers there is a marked absence of room to negotiate a privacy policy. Teleologically, this assessment could prove to be very helpful for private users who do not wish their aggregated data are used for big data analytics. For the purposes of this Article, Figure 1 (the table used by the German FCO in her anti-trust investigation of Facebook) is illustrative. It shows the nexus of contracts between Facebook, its private users (top right) and several third parties.

[**Figure 1**, © courtesy of the Bundeskartellamt, 7 February 2019]



[34] Bundeskartellamt, case B6-2216, 7 February 2019 (FCO 2019). See, *infra*, para. 1.4. At the time of closing this paper, the ruling was subject to appeal. It is very likely that the appeal will take place.
[35] "Private users" is the terminology used by the FCO. "Germany Restricts Facebook's Data Gathering", *NYT*, 7 February 2019. The commentator Labeled as a "novel anti-trust argument."
[36] By the summer of 2019, Facebook claimed to have modified its privacy policies.

Figure 1 presents the data streams from the platform provider.[37] It is immediately clear that private users *cannot* be aware of the purpose and full scope of the data that is submitted to, assembled and generated by the platform provider. The only direct legal link for the private users with the digital platform provider is the arrow that goes to and from Facebook. In practice, there are at least three more links from the private users: to developers, publishers and advertisers. The private user is unaware of what these parties do with their date, as there are no transparent terms or conditions of data use governing the contractual relationship between developer, publishers or advertisers who are active on the digital platform.

No matter the dark and sinister aims of CA, it was Facebook that transferred the data to CA – under the pretext of a having imposed a legally binding DTA.[38] Ultimately, Facebook became subject to legal scrutiny by several authorities.[39] In terms of creating trust and control for big data analytics the question is: if a digital platform provider shared and transferred personal or aggregated data of hundreds of thousands private users, how did it inform them? Would this right to transfer data be implied in a privacy policy or general terms and conditions? What rights, if any, were granted to the platform's private users whose source data – whether or not with the use of pseudonymization – were shared with third parties? Were these private users made aware sufficiently how to enforce their rights? What do personal data/privacy policies provide in terms of the platform provider sharing and transferring data to a third party for the purpose of big data analytics?

1.5 Just another boring set of personal data policies?

[37] The German FCO ruling is concise and very instructive. As regards CA: it was a US affiliate of a privately owned British company that specializes in the provision of data mining, data analysis and direct marketing services for application in the domain of public election processes. See, e.g., Linnet Taylor, "In the digital world we are all developing countries: what Cambridge Analytica can tell us about limited statehood in the West," in: *big data, justice*, internet article, 22 March 2018, https://linnettaylor.wordpress.com/category/big-data/. (Taylor, 2018) The company no longer exists. A criminal investigation was running against some the company's executives in 2019.

[38] For the sake of clarity, this Article uses the generic notion of data transfer, since that is what occurs in practice, and the agreement itself will contain scoping arrangements.

[39] CA and Facebook were one focus of and enquiry by the ICO into data and politics, see also *The Guardian*, 17 March 2018. See also the investigation into politics, https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/.

Private users are data subjects. Although there are several transparency enhancing tools for privacy policies available, private users, at most, browse through privacy policies, when accessing a digital platform and purchasing services online.[40] This may have to do with several circumstances: (1) most data policies look the same, which makes the private users less vigilant; (2) data policies tend to be light on controller/processor obligations, and they are almost always non-negotiable; and (3) data policies tend to contain more disclaimers and controller rights than data subjects' rights. These circumstances may be a hurdle private user, as they feel there is nothing they can do. In the data economy, consent is key, yet there is a good chance of platform providers by-passing the consent requirement, given their hunger for amassing data for analytical or other commercial purposes. In addition, the manner in which privacy policies are presented does not point at establishing a direct legal connection between the private user and the platform provider.[41] The private users lose track of the policies that apply to them. Often, they are unaware with whom they are contracting. The high level statements beg the question for the private users who do read and understand a policy: "*How can I actually enforce any rights against the platform provider?*"[42]

The requirement of asking for (explicit) consent was never intended to bring long, impenetrable privacy policies. Nor was it designed to mean in practice that any data subject on social media would have the choice between either consenting or not getting access to a service she desired. Consent implied that the data subject would be able to form a clear understanding of her rights. Compare this with general terms and conditions. These will have to be adhered to if the private user has implicitly or explicitly accepted them. The law offers various options to void or nullify terms that are blacklisted or grey-listed. GTC may be set aside should the private user not having been offered a reasonable opportunity to take note of their content. Besides, GTC are not unilateral compliance statements. There is a two-sided contractual relationship.

The publications on the CA backlash did not reveal immediately what type of contract Facebook and CA had entered into. The private users/data subjects had not been informed properly of the purposes to aggregate personal data and match them with

[40] See *Eurobarometer Special 447 on online platforms* (2016).
[41] *Supra*, Figure 1.
[42] H.U. Vrabec, Uncontrollable Data Subject Rights and the Data-driven Economy, dissertation, University Leiden, 2019 (Vrabec 2019).

other (personal) data – often in the circle of trust of the first data subject. The private users could not ask CA or Facebook to cancel the process. Neither party offered transparency to any of the private users on CA's processing and analytics methods and purposes either. In the press there seems to be a consensus that, at some point, Facebook demanded that CA delete the accumulated data of Facebook's private users. Yet there also seems to be consensus that, not only did Facebook not follow-up on its demands against CA; it chose not to inform affected users proactively. According to its own policies, the only obligation Facebook had was to require strict confidentiality from CA. Having gone over the applicable policies in February 2018, it seems that the legal basis for sharing data with third parties hinged on the following two statements:

> "*Sharing With Third-Party Partners and Customers.*
> *We work with third party companies who help us provide and improve our Services or who use advertising or related products, which makes it possible to operate our companies and provide free services to people around the world.*"

And the following clause in its Data Policy (emphasis added):

> "*We transfer information to vendors, service providers, and other partners who globally support our business, such as providing technical infrastructure services, analyzing how our Services are used, measuring the effectiveness of ads and services, providing customer service, facilitating payments, or conducting academic research and surveys."*

This provision was supplemented with a conveniently vague addition:

> *"These partners must adhere to strict confidentiality obligations in a way that is consistent with this Data Policy and the agreements we enter into with them.*"

The above texts do not match reality. Did Facebook even agree on strict confidential obligations with CA? What agreements was Facebook referring to? More policies followed: considerations and a justification of Facebook submitting masked or aggregate personal data to third party companies. Facebook reassured that not the user's personal data, but "*non-personally identifiable information only*" would be shared with third parties;[43] these data would be shared "*for analytical purposes*".

[43] The correct definition would be whether the data would or would not: "(…) *relate to 'an identified or identifiable natural person'*. Confer with the GDPR, recital (26).

From a contractual perspective the question is whether a digital platform provider can be held accountable directly by its private users for not enforcing against a third party the "*strict confidentiality obligations*" it mentioned in its policies.

2. THE DATA ECONOMY, DIGITAL PLATFORMS & BIG DATA ANALYTICS

2.1 A big data economy while controlling data on digital platforms?

The regulatory focus on digital platforms is without prejudice to the rules related to the protection of personal data. How does that help private users subjected to big data analysis? The Commission's functional approach focus is devoid of any vision on empowering private users in enforcing their rights in civil courts. See, *e.g.*, the principles (art. 5) or consent provisions (art. 7: consent resembles offer/acceptance). The data subjects' rights are set forth in Chapter III GDPR, effectively and directly against the controller or various (sub-)processors. The problem present in parts of the GDPR is that not all controller/processor obligations are matched with data subjects' rights and that they are not transportable to big data applications. Where they are – section 3, articles 16 (rectification) and 17 (erasure), article 18 (restriction on processing), article 20 (data portability) – the rights are often qualified and the burden of proof is not clear. Article 79 GDPR opens the door to various legal remedies, including administrative or non-judicial remedies, in the Member States.[44] Article 82 contains provisions on compensation and liability in case the personal data rights of the data subject have been breached.

This could be the procedural law nexus with private law. To study the effectiveness requires more GDPR case law analysis. Some of the material provisions appear not easy to enforce: section 4, the right to object and automated individual decision-making (articles 21-22 GDPR) contains fairly complex exclusions that are not explained in detail in the extensive considerations.[45]

[44] See also Article 79 (2) on the competent court: "Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers."

[45] The GDPR contains only three considerations (20, 71 and 125) and they deal with varied issues.

Another question is how the GDPR connects with the Free Flow of Non-Personal Data Regulation. The latter is lays down rules relating to data localisation requirements, the availability of data to competent authorities and data porting for professional users. *Prima facie*, these are rather fragmented and specific regulatory objectives. The definition of what are non-personal data leaves much to be desired.[46] Rather than defining what non-personal data are, the Regulation provides some examples:

> *"Specific examples of non-personal data include aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines."*[47]

Article 6 draft Free Flow of Non-Personal Data Regulation – the provision on data porting – stipulates that the Commission must encourage service providers and professional users to develop and implement codes of conduct detailing the information on data porting conditions (including technical and operational requirements) that providers should make available to their professional users in a sufficiently detailed, clear and transparent manner before a contract is concluded. The Commission will review the development and effective implementation of such codes within two years after the start of application of the Regulation. The objectives of achieving a general right to data portability for non-personal data, a right to data access and liability for data (mis)use should be viewed in context. The Commission considers a data portability right first as a means to enhance competition, stimulate data sharing and avoid vendor lock-in. The underlying thought being that data access and liability will support data portability. The Staff Working Document displays the Commission's thought and concerns regarding liability, with mention of big data analytics.[48] The considerations on possible liability for damages resulting from unlawful data analytics are at a high level of abstraction. No thought is given on how damages claims would have to be enforced. Discussions may range from legal issues regarding contractual, extra-contractual to risk liability. Liability concerns must be capable of being translated in clear, relatable and achievable policies that offer recourse to private users who suffer damages as a result of non-personal data being transferred or processed.

---

[46] *Cf.* art. 3 of the Non-personal data Regulation: "'data' means data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679;"
[47] Consideration (9) of the Free Flow of Non-Personal Data Regulation.
[48] Commission Staff Working Document 2017, p. 40*ff*.

It will be challenging to align the different objectives and interests. There may be another dichotomy in the working, as may be inferred from the mid-term DSM strategy review.[49] The Commission wants to simulate data flows *and* it wants digital platform providers to inform their users more effectively what personal information and data is collected and how it is shared with and used by others.[50] The analysis of the proposed instruments reveals a lack of a vision in terms of the economic value and model for big data analytics, their importance for the EU economy and the possible pitfalls. The prime example for the purpose of this article was discussed above: big data analytics are not supported by clear, enforceable data analytics agreements nor any codes of conduct. Perhaps this is due to the circumstance that, with the exception of the Free Flow of Non-personal Data Regulation, the principal plans on stimulating the data economy are under construction. It appears unlikely that data mobility and data portability regulation across the Union is going to improve under a Free Flow of Non-Personal Data Regulation. The current wording is not very clear and sustainable. It balances the different interests of the stakeholders.

2.2 Data mobility: control & trust

The tracking of online activity has become a revenue model for Internet service providers (ISPs) and data analytics companies. This development begs the question whether big data assembled from online tracking should be considered personal even where anonymisation techniques have been applied. The reason is clear: it is likely that it is not that hard for the data analytics processing company to "*infer a person's identity by combining allegedly 'anonymous' data with publicly available information such as on social media*".[51] In the Communication on Online Platforms and the DSM the Commission outlined the pros and cons.[52] A concern is that the digital platform providers may have an inherent conflict of interest: while they play a key role in digital

[49] Commission Communication DSM 2017. On page 2, the Commission mentions a number of different activities ranging from: online advertising platforms, marketplaces, search engines, social media and creative content outlets, application distribution platforms, communications services, payment systems, and collaboration platforms.
[50] Currently Directives 95/46/EC and 2002/58/EC and once applicable, the GDPR.
[51] EDSP 2015, p. 7.
[52] Commission Communication "On Online Platforms and the Digital Single Market – Opportunities and Challenges for Europe", {SWD (2016) 172 final}, *COM (2016) 288 final*, Brussels, 25.5.2016 (Commission Communication 2016).

value creation, there is a blurring between service provision and the creation of significant value through data accumulation. Rather than considering what the implications may be for data analytics processes, the Commission refers to the GDPR only, and then considers the benefits of data analytics for its own goals of ensuring "*a data-driven public sector."* [53]

Articles 4, 25 and 32 GDPR[54] and the consideration in the draft Free Flow of Non-personal Data Regulation that personal data regulation remains applicable are meant to safeguard that enhanced data for big data analytics purposes cannot be decompiled to reconstruct the personal data input.[55] Article 25 GDPR provides the regulatory requirement that must precede any form of big data analytics. The controller must consider issues such as the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing. The general requirement that it must implement appropriate technical and organisational measures applies as well. Article 32, (1) (a) extends these to "(a) the pseudonymisation and encryption of personal data." Article 4 (5) GDPR emphasizes the definition of "pseudonymisation" to facilitate big data analytics by using data minimisation.[56] From a perspective of personal data regulation, there is a depository to build the big data economy on, plus a privacy check prescribing data minimisation. Yet, more reliance on – and verification of – contractual arrangements between the digital platform service provider and the data analytics company may be necessary. No matter that many big data processes do not always include personal data processing: big data analytics involve novel, complex and sometimes unexpected non-transparent uses of personal data.[57] it is necessary to have the parties involved make a privacy impact assessment (PIA) beforehand in light of providing accountability to competition and data authorities. Elements of the PIA

---

[53] JRC/IPTS Digital Economy Working Paper "An economic policy perspective on online platforms", 2016 (Digital Economy Paper 2016).

[54] See GDPR, recital (26).

[55] Article 40 GDPR prescribes a code of conduct.

[56] "'*pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject <u>without</u> the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.*"

[57] *Cf.* EDPS 2015. The European Data Protection Supervisor made it crystal clear that big data obtained through online tracking should still be considered personal even where anonymisation techniques have been applied. The reason is simple. It is easy infer a person's identity by combining allegedly 'anonymous' data with publicly available information from social media.

could include investigating whether the processing is fair; to what extent it could affect data subjects; and to determine measures to mitigate impact and strengthen control.

For the above reasons – lack of trust and no clear view yet on liability issues – the EU institutions are concerned about the loss or lack of control by the data subject. The Commission seems to think that detailed regulation could clash with the desire to stimulate the DSM. However, trust is key. There are two levels of trust: (1) trust by private users in the processing of their personal information by digital (or online) platforms, *and* (2) trust between a digital platform service provider, who enters into a form of contract with a third party service provider, who will perform big data analytics using data assembled by the digital platforms provider.

2.3 Control of big data contracts?

If the data protection authority in a Member State would have a right to verify the contents of the DTA and impose changes and perform checks on purpose limitations and accountability, this could create more trust and control. But first, a look at the stakeholders in figure 2:

(1) Private users of the digital platforms – even if the personal information they supply may not always be personal data;

(2) Service providers on the digital platforms – whose business models may still be built on free access against data use;

(3) Big data analytics companies, who take data, use AI to enrich them and provide them as a paid service to other the service provider or third parties, and

(4) Clients who want to use the output of the analysis for scientific, medical, statistical and many more (some not very altruistic) purposes, want to know whether they own the data.

Figure 2 attempts to illustrate some of the dichotomies.

User: personal data > Platform service provider > Data analytics company
Transparency
| = Trust * | = Control
Source: Privacy / Data Use Policy < - > Data Transfer Agreement **|** **Codes of Conduct**
Non-negotiable Terms & Conditions * Contract negotiations: scoping **Purpose, obligations, liability**

Figure 2 Regulatory Compliance and contracts for big data

Perhaps the debate should focus on whether, and if so, how data can qualify as a species of property. However, especially in the United States, there seems to be quite a lot of opposition to "*mix property concepts with privacy concepts.*"[58] Even though personal data protection undeniably seeps through in commercial big data analytics, would the academic debate be better off by not just looking at big data analytics from a trust and control perspective, but also from an economical contract law perspective? When considering how private law may function as a control mechanism for enforcing regulatory requirements, the question of data ownership arises. Who owns data? If a user *owns* her personal information, would that entail that she can do whatever she desires with those data? Could ownership function as a lever on giving consent to digital platform providers? If a client instructs a large and expensive big data analytics project, should it have all the freedom to keep the data output exclusively for its own purposes? Which stakeholder should have the economic rights in the provided data; the enhanced data; the analysed data? These questions will be discussed in para. 3.

3. QUALIFYING (BIG) DATA AS PROPERTY & OWNERSHIP

3.1 Law of Property Notions

Western legal systems are founded on the notion of property ownership, or law of property. But so far, data have not been qualified as property in most if not all legal systems. Data as a commodity keeps growing. It was also discussed that regulators

[58] W. McGeveran, "Big data and privacy: making ends meet", *Conference Paper*, 2012 (W. McGeveran 2012).

acknowledge the importance of a data economy.[59] Both input and output data are considered as valuable currency. The question would then be which persons (whether legal or individual) should benefit economically from the income generated by processing and analysing data. A further question most likely would include the distribution of the income. Who would be entitled to data income? What if there is chain of events – as is the case with CA – and what role could contracts play at different levels? These are key questions. But it is challenging to qualify data. Data can be anything, from files to location or traffic data, to IP addresses, log files, credit card files, or search terms; they can be digitized music, images or words. Data as such is an abstract notion: one cannot hold data in her hands. But the scope of data continues to widen. Can one give data as a present? For these purposes a durable data carrier used to be required, but that may no longer be the norm. The distinction between digital data, their storage – on which business cases are also built – and the underlying information characteristics at the basis of the database blur more and more as well.

There are negative aspects to the data economy. It seems that using output of data analytics commissioned by companies blurs the fundamental right to privacy; and to a high level of consumer protection as well.[60] Thus, an undesirable lack of nexus in the treatment and qualification of data in the context of personal data protection and the treatment and qualification of the same in the context of their economic value may occur.

In this paragraph, the intellectual property approach to data will be discussed briefly.[61] The justification for mentioning IP is that there is a piece of regulation in the EU that contains element of database ownership. The requirements for intellectual property protection – a form of originality – may turn out to be an unsurmountable obstacle when it concerns enormous collections of data that may have been enhanced by algorithms. Let it be reiterated that this Article is concerned with ownership by private users who provide the underlying data for processing by an unknown third party and for unknown purposes. Bringing private users data ownership in this context under the scope of intellectual property rights probably would require the defunct *sui generis* debate to rise

[59] *Supra*, paras. 1.1 and 2.1.
[60] Art. 38 EU Charter of Fundamental Rights; art. 169 (1), 169 (2) sub (a) TFEU.
[61] B. Van Asbroeck, J. Debussche, J. César 2017-1, p. 59-110.

again like a phoenix. Clearly, there is a pragmatic, but misty approach to data assembled by platform providers. The Commissioner who was in charge of consumer rights until 2019, promised action to make the business models of platform provider more transparent in their general terms and conditions.[62]

There are pros and cons in qualifying data as property. As simple legal pragmatism, data as property aligns economic hopes with private law measures. This alignment, with some regulatory invention on abuse of personal data, support a case for bringing personal information in the realm of generic property law. Similarly, this could be argued for data output as well. As the digital transformation is becoming irreversible and where data protection regulation does not provide full protection of digital data floating around outside the control of the private users/data subjects, a new approach to data ownership is inevitable.[63] The notions of intellectual property or *sui generis* rights focuses on rights for parties who have invested in building databases.[64] It does not match with the current practices on digital platforms. Moreover, the EU Database Directive has proven to be unsustainable. It does not address the existence of an underlying right on the actual data in detail.[65] Neither does it clarify the main protection mechanism – copyright – nor the *sui generis* right, which was dead on arrival.

---

[62] See Commissioner Vera Jourová, European Commission – *Press Release*, "Facebook changes its terms and clarify its use of data for consumers following discussions with the European Commission and consumer authorities", Brussels, 9 April 2019 (Commission/Facebook Press Release 2019); and "Facebook promises more openness after an intervention by ACM", *Het Financieele Dagblad* 10 April 2019, (translated from www.acm.nl/nl/publicaties/facebook-past-voorwaarden-aan-het-voordeel-van-consumenten, www.acm.nl/nl/publicaties/facebook-past-voorwaarden-aan-het-voordeel-van-consumenten: ACM is the Netherlands Competition Authority).

[63] For other perspectives see, *i.a.*, Determann 2019; H. Richter, P.R. Slowinski, The Data Sharing Economy: on the Emergence of New Intermediaries, *ICC International Review of Intellectual Property and Competition Law*, Vol. 50, Issue 1, pp. 4–29, January 2019 (Richter, Slowinski 2019).

[64] Think of (1) updating and adding new elements, data enrichment, applying hardware and tools not only to store but also to unlock data assembled and providing for safe carriers; and (2) exploitation of data would include granting user licenses to third parties, transferring data for money, or data as currency.

See, e,g., B. Van Asbroeck, J. Debussche, J. César, "Building the European Data Economy, Data Ownership, A new EU right in data", *White Paper*, Bird & Bird, 1 January 2017 (B. Van Asbroeck, J. Debussche, J. César 2017-1), p. 17-26. (E. Tjong Tjin Tai, "Data and the law of property", *WPNR: Weekblad voor Privaatrecht, Notariaat en Registatie* [in Dutch], 149 (7085), 993-998, 2015 (Tjong Tjin Tai 2015), p. 994*ff*. See also the English submission by E. Tjong Tjin Tai, "Data ownership and consumer protection," *Tilburg Private Law Working Paper Series*, No. 09/2017.

[65] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *OJ L 77,* 27.3.1996, p. 20–28 (Database Directive 1996). The Directive created a new exclusive "sui generis" right for database producers, valid for 15 years, to protect their investment of time, money and effort, irrespective of whether the database is in itself innovative ("non-original" databases). The Directive harmonised also copyright law applicable to the structure and arrangement

The Trade Secrets Directive supports the argument that (business) data should be treated as property.[66] It is intended to complement the intellectual property rights regime. The notion of trade secrets could perhaps and to some extent be applied to commercially valuable data and information that do not qualify for intellectual property protection. As such, the protection could be akin to the *sui generis* protection afforded under the database directive, if not for the fact that the object of protection is a database and not the data. The key requirement is that the data are kept secret. As such, the party that controls the trade secrets is required to undertake reasonable steps to protect them.[67] Once the data have been analysed and are published as big data, there is no trade secret anymore. In sum, it is unlikely that a trade secrets approach to big data would yield any functional result.

The fact that the Commission has an eye for data processing rights in the context of intellectual property rights does not mean data could be qualified as property. Indeed, the formulation in the Proposal on Copyright in the DSM turned the notion on its head: text and data mining of copyrightable material was to become a mandatory exception to the copyright ownership – in the context of temporary reproduction acts.[68] Hence, this upside-down definition is not helpful either.[69]

Since database regulation does not work in the ownership discussion, the focus must be on data as property.

3.2 Data property law?

Probably as a consequence of legislators having cold feet in addressing this fundamental issue, there is no EU or Member State's approach to the qualification of

---

of the contents of databases ("original" databases). The Directive's provisions apply to both analogue and digital databases.

[66] **Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure,** *OJ L 157,* 15.6.2016, p. 1–18.

[67] See Article 2 Trade Secrets Directive.

[68] The EU Directive on Copyright in the Digital Single Market, COM 2016 (593) final (at the time of closing, it was still not final), which amends both the EU Copyright Directive of 2001 (2001/29/EC) and the Database Directive (96/9/EC).

[69] B. Van Asbroeck, J. Debussche, J. César 2017-1, p. 72-75.

data as property in some form yet. There is little case law,[70] and there has been an ongoing academic debate on the data property issue.[71]

It is not easy to imagine the legal qualification of the commercializing of data under private law. Many questions arise. How to vest a mortgage on data? How to calculate their economic value? Should the provider of the mortgage have a physical data carrier? Should it be possible to update the data on a carrier? If the data needs to be updated, how often? How to define the parties are, when there is no contract? These questions reveal the problems that may be caused when considering data as intangible goods, and the data carrier as a tangible good. It no longer makes sense to determine the carrier to be the decisive good, as data is digitized.

Subsequently, if data can be easily reproduced and retransmitted,[72] is it relevant to determine who qualifies as the first 'owner' of the data?[73]

The data policies display the difference between the two very different notions of data that have developed over time: data meaning personal data that are protected under privacy law versus data meaning a good that does or does not qualify for ownership. The difference becomes visible in the sad reality of many controllers using hollow privacy and data policies in terms of providing protection to the data subject as compared to parties who, *e.g.*, develop data in a data base or acquire (personal) data through a transaction for commercial purposes.

The fact that there is no EU shared view on zero harmonization of the legal status of data under property law does not prevent the Commission from voicing that data ownership is a hot topic. Yet, the debate does not align the interests of data subjects with the private law qualification of data. The Commission focuses on data property solely as being an internal market issue. The Commission acknowledges that there may be a regulatory gap that could cause harm:[74]

---

[70] An early and not entirely convincing example can be found in a decision of the upper court of Karlsruhe going back to 1995 and that related to the destruction of data: OLG Karlsruhe, Urt. v. 07.11.1995 – 3 U 15/95 – *Haftung für Zerstörung von Computerdaten.*

[71] *Cf.* B. Van Asbroeck, J. Debussche, J. César 2017-1, p. 17 and p. 22-25.

[72] So can software, but if satisfying the originality criterion, and subject to the exclusions and exhaustion doctrine, software will fall under the protection regime.

[73] *Cf.* Tjong Tjin Tai 2019, p. 10ff.

[74] Commission Communication on Towards a Thriving Data-Driven Economy, COM (2014) 442 final.

> "*Barriers to the free flow of data are caused by the legal uncertainty surrounding the emerging issues on 'data ownership' or control, (re)usability and access to/transfer of data and liability arising from the use of data*."[75]

The scope of information is the basis for the processing. That basis may or may not lead to a qualification of data as an absolute property right.[76] Where the harmonization of private law in the EU is not proportional and may clash with the principle of subsidiarity, could there be room for zero base harmonization?

Conceptual problems appear to abound. A problem is that property is any interest in an object, tangible or intangible, that is directed against everybody (the *erga omnes* effect).[77] Exercising control over one's 'own' data is something different from 'owning one's data.'[78] The *erga omnes* effect may be aimed at certain stakeholders only. Hence, it may be less effective.

Another problem is that, without a proper qualification of the nature of data (para. 3.1), contract law would support probably only *the way in which* the data might be exploited. This writer is not in favour of such a top down approach: definitions of ownership to determine whether data can be property. Ownership should be the result of there being a property; not the other way around.

A third problem is that in privacy law, control is a term does not apply solely to a data subject. Linguistically, control applies to data processing by the controller. Under private law, control must also be exercised in the data subject's realm. Control should not be restricted to the digital platform provider or the client's use of the platform.

The fourth problem is that legislation in civil law countries and case law in common law countries considers property law as a closed system. It not easy to define a new type of good under property law, be it personal information or the outcome of a data analysis. Courts in common law countries have offered an opening to qualifying property law as a restricted rather than a closed system:

---

[75] Commission, "European Free Flow of Data Initiative within the Digital Single Market" (Inception impact assessment, 2016) <http://ec.europa.eu/smartregulation/roadmaps/docs/2016_cnect_001_free_flow_data_en.pdf>

[76] Compare the French Code Civil, article 544: "*La propriété est le droit de jouir et disposer des choses de la manière la plus absolue (…).*"

[77] See N. Purtova, 2011, for a theoretical discussion of property rights in personal data (Purtoya 2011).

[78] Other than that the GDPR considers it a desirable trait: see recital (7): "*Natural persons should have control of their own personal data*," and: "*Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.*"

> "*Before a right or an interest can be admitted into the category of property, it must be (i) definable, (ii) identifiable by third parties and (iii) have some degree of permanence or stability*."[79]

It appears that the third requirement – permanence and stability – might not be satisfied that easily on a digital platform. Consider the case of online tracking of information on social media: beyond the ownership question lies the question whether the personal data that are being mined are more of a fleeting, or of a stable presence. Yet, perhaps this should not be an insurmountable problem. Most data are stored on a stable carrier – and that includes, in my opinion, data on a server.

Once this obstacle is overcome, there is the need to bring data into a defined category of property. Examples are movable and immovable property; material and immaterial property; tangible and intangible property. The negative starting point is that data cannot be considered goods, since – without a carrier – data are not capable of materiality. In common law, some scholars have opined on the need to treat data as a proprietary law issue. Property is often defined as "a bundle" of rights and obligations rather than emphasizing the materiality. This approach makes sense.[80] The data carries the economic value, not the data carrier or database. Without the data these carriers are empty shells:

> "*That is to say that the protection of the economic value inherent in personal information should be grounded in property rights acknowledged by the law*."[81]

A fifth theoretical problem regarding the qualification of data under private law is that it would be difficult for the owner to warrant exclusivity of the data and the database – data can be copied easily and infinitely as was established above. Besides the fact that this argument was used in the discussion of the protection of software – and was overcome – the fact that the owner can make the data available to many different processors or users does not stand in the way of establishing it as a property. Developments in the exploitation of big data, their manageability by different

[79] Judgement in National Provincial Bank v Ainsworth [1965], AC 1248, opinion by Lord Wilberforce, cited in C. Rees (2014), p. 77.
[80] Tjong Tjin Tai 2015, p. 995, who refers to G.S. Alexander, E.M. Peñalver, *An Introduction to Property Theory,* Cambridge: Cambridge University Press 2012 (G.S. Alexander, E.M. Peñalver 2012).
[81] Rees 2014, p. 2.

stakeholders simply require a functional approach: in this way data are, at the least, comparable to goods.

The pragmatic approach to the qualification of data as property requires answering what private law aspects matter in data ownership. First, the right of use; second a form of control exclusivity of the party who exploits the data; third, the right to dispose of the data; and fourth, rights and obligations that may be attached to the data, *e.g.*, the possibility of liability for their content, or the right to claim the ownership of data that are in the possession of a third party.[82]

Finally, the question of enforcement of data ownership. How would that work? Art. 79 GDPR contains a choice of forum to facilitate data subjects to enforce their rights under the GDPR.[83] Perhaps private law should not simply complement the enforcement of data protection law. Neither should data protection law supplement private law. Both data protection regulation and private law have in common that they aim at embedding trust and control of data.

The regulatory gap that may arise is the result of overlapping, mixing or exclusionary administrative law and private/consumer law rights and obligations. Private users are served by complementary rules; not by discussions regarding competences, or different interpretations of material legal provisions.

A starting point for embedding personal information in property law contracts is that it should not merely consist of a replication of the models for personal data protection.[84] Some scholars – in the US – distinguish between rules on property, and rules on liability – without addressing whether this is a matter of law or contract.[85] Or, as Lessig clarifies:

> "*The key to a property regime is to give control, and power, to the person holding the property right.*"[86]

---

[82] For a bottom-up approach to personal information as a case study for property law, see J. B. Baron, "Property as Control: The Case of Information", 18 *Mich. Telecomm. Tech. L. Rev*. 367 (2012) (J.B. Baron 2012).
[83] *Supra*, para. 2.
[84] B.J. Evans, "Much Ado About Data Ownership", 25 *Harv. J.L. & Tech* 69, 2011 – in the context of patients' privacy protection.
[85] G. Calabresi, D. Melamed, "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral", 85 *Harv L. Rev.* 1089 (1972).
[86] L. Lessig, *Code and Other Laws of Cyberspace* 160 (1999).

It makes sense to look at the exercise of ownership first: what rights would accompany the data property?[87] The exercise of exclusive rights over the data property would fall into: rights which are exercisable in personal information against everybody *(rights in rem*, *i.e*, rights that are associated with a property and not with a personal relationship) and more limited: rights *in personam*, (i.e., rights which are attached to one's persona). Rees writes:[88]

> *"The ownership paradigm will encourage the use of privacy enhancing technologies and state of the art security measures to protect data. Those who hold vast quantities of personal information will realise the risks inherent in losing the property of vast numbers of third parties and the risk of consequent class actions for damages for having done so."*

It is an open question whether ownership should have the nature of an exclusive or a non-exclusive right. This requires further scholarly debate on the intersection between property law and the desire to stimulate through regulation the European data economy.

Another complication in allocating data ownership lies in the fact that, in practice, different third parties and the algorithms or other analytical tools they apply, may be involved in various stages of the data analytics process. This creates an extra issue that is best avoided: agents or subcontractors claiming big data (joint) ownership. It would make economic exploitation of the data more difficult and the legal standing of the private user weaker. Under property law – joint ownership is likely to create legal issues as regards the exercise of exploitation rights and the enforcement of data ownership rights. A possible solution for this is provided in the Data Ownership White Paper. The solution entails imposing a "traceability obligation" on the transferee who engages in the big data processing.[89] This obligation would entail that the transferee must keep logs of all steps in data processing for the performance of data analytics. Or: which party has done what with the data, what did their efforts result in, and, thus, why are they the owners?

Still, once we are willing to agree that data ownership as a legal concept would serve to support both trust of the private user in the aggregating and processing of its personal data and control by the platform provider in data transfer agreements, we

---

[87] C. Rees 2014, p. 78.
[88] C. Rees 2014, p. 79.
[89] B. Van Asbroeck, J. Debussche, J. César 2017-1, p. 125-126.

face another legal question: how to ensure that the two-step transfer approach creates trust when there are *hundreds of thousands* owners party to one agreement? *Prima facie*, it seems that the practical way forward would be to give the platform provider a form of proxy to negotiate the terms of the data transfer agreement on behalf of the data subjects. But, that requires trust in that provider.

The qualification of (big) data under private property law notions may be an unresolved matter that requires further extensive legal research. Notwithstanding this need for research, some academics, including this writer, argue in favour of a functional and more open approach to exercising control and trust over data that have been either offered or generated by private users/data subjects. Consequently, a more detailed perception of private law options to exercise ownership rights should be (re-) considered. In this approach, consumer law notions barge in as well.

A different approach, focused on the contractual enforcement of rights, may be wise. In terms of big data analytics agreement between the platform provider and a third party, the policies leave much to be desired, and the private users must adhere to regulatory authorities rather than courts to adhere their rights.[90] This begs the question whether consumer rights could offer protection of private users.

3.3 Contractual regulation & consumer rights: transparency

The contractual description of what the data are and how they may be processed fairly is part of a functional approach to protect rights both of the party who desires to transfer data ownership (transferor) to another party (transferee) pursuant to a fair contract *and* any data subject at the source of the transfer. In literature focusing on data governance, the focus is on fairness of and accountability for processing, plus transparency. This paragraph discusses transparency as a legal norm.

Freedom of contract should be available for private users to negotiate their own terms in a DTA. Yet, the freedom of contract seems to be far away. Besides there is a lack of transparency on how the processing of data is performed.[91] How to secure transparent data transfers? Transparency can be considered from three perspectives: (1) The linguistic perspective provides to what extent the meaning of a word or idiom

[90] *Supra*, para. 2.1.
[91] N. Helberger, F. Zuiderveen Borgesis, A. Reyna 2017, p. 1430*ff*.

can be deduced from its parts. This means that when a word is split any part of the word can be traced to the meaning (e.g., Blueberry, a berry which is blue);[92] transparency of data collection, transfer is simply what it means. (2) The economic perspective is aimed at very different considerations. A market is transparent when it provides a clear insight into the price, quantity and location of products, services, and/or capital goods. Transparency then is a condition for a free and efficient data market.[93] In my view, economic transparency should include sharing, transfer and processing transparency; (3) the legal perspective of transparency is quite broad. The scope of transparency must thus be seen in the legal context. Recital 58 GDPR provides a definition; data ownership is a complex notion that is not easily applicable in private law. Within private law, consumer regulation applies transparency as a norm without clear delineation.[94] Hence, a custom-made approach to transparency of big data analytics may be required.

The use of a clear, enforceable, and transparent DTA serves to delineate the scope of use by the third party (transferee) of the aggregated data. Whether the transferee acquires a form of ownership in big data produced could be a matter of contract discussion. As is the case with a license agreement, the scope of use can be as limited or as extensive, as the parties agree. The scope is dependent upon the activities to be undertaken by the transferee and whether the cooperation between transferor and transferee qualifies as a service or more a cooperation agreement.

Conversely, the transferee wants to delineate what it can do with data transferred to it. Possible scope of use and purpose could include the right to aggregate, reproduces, modify, mask, filter, enrich, combine, merge or partition data. Whether the transferee is entitled to share, make public, outsource parts of the data or even delete the data must be considered carefully by the transferor.

For at least two reasons, it is important that the DTA contains provisions on rights for the transferor versus the third party to: (1) audit and inspect the terms of big data

[92] One definition provided by the Cambridge Dictionary and often copied in other linguistic definitions is: “the characteristic of being easy to see through.” See also: E. Sherko, “Linguistic Transparency and Opacity in Compounding,” *Acad. J. Interdiscip. Stud.*, vol. 4, no. 3, pp. 590–593, 2015.
[93] See, generic literature, such as J. Smullen and J. Law, *A dictionary of finance and banking*. Oxford University Press, 2008.
[94] Transparency is mentioned in various contexts in the Online Intermediary Services Regulation, without any definition.

processing, (2) govern and control the scope and purpose of the processing, and (3) ensure accountability by the third party:

- The personal data regulation requires for the transferor to apply the GDPR to DTAs; and
- The transferor must be able to verify and contest the big data output.

In reality there is not much verification of big data output. Yet, the inclusion of contractual obligations could enhance the position of the private users. Examples are the implementation of technical and organisational measures to address matters such as data security, data minimisation and data segregation. If the goal is to empower private users on digital platforms to get more control over and have more trust in the pseudonymised data that have been aggregated and used for big data analytics purposes, then there is no reason why this could not be achieved bottoms-up from a consumer law perspective (the complementary approach).[95]

From a private law perspective proportionality of the contract provisions and tailored transparency obligations should be considered. Digital platforms are required to use clear and easily accessible terms and conditions of their services. They should provide also a statement each time they decide to suspend or terminate the use of their services by a private user. Embedding equivalent legal obligations for big data analytics in general terms and conditions is a possibly effective regulatory measure. The principle of transparency – or information provision – could prove to be a palpable solution for private users on digital platforms. Case in point: the Online Intermediary Services Regulation.[96] In spite of lacking a legal definition, the Online Intermediary Services Regulation presents a few meaningful obligations that could be imposed also on the big data analytics providers either directly or indirectly through the digital platform providers. And the Regulation contains a transparency requirement: digital

[95] The GDPR contains a solution regarding locus and basic rights in art. 79 – but it goes against enabling consumers to go either one or both ways, when their data are compromised.

[96] Not to be confused with the draft Digital Content Directive from 2015; see: Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content COM(2015)634 final, referred to by N. Helberger, F. Zuiderveen Borgesius, A.Reyna 2017, has not passed the legislative process yet. By January 2019, the Commission mentioned that a political compromise (which seems to grant a bit more protection to the suppliers, i.e., digital platform providers). had been reached.

platforms providers are required to use clear and easily accessible terms and conditions of their online intermediation services.[97]

It should be borne in mind that there is no nexus between the private user and the third party (transferee) who obtains data from the platform provider. Providing transparency on the use of data – or their place in the business model of the platform provider – is a behavioral requirement that grants the private users control over the data use originated by the digital platform providers.[98] It could also enhance the private users' trust in their providers.

But still… If the nexus is between the private users and the digital platform provider and between the digital platform provider and the third party, there continues to be a lack of harmonization of European contract law. The private users are protected against the platform providers, but, not against the third party. The 2011 Consumer Rights Directive contains very few personal data-related provisions benefitting consumers.[99] Probably, meaningful protection provisions for the private users could be taken from the Online Intermediary Services Regulation and the Unfair Commercial Practices Directive.[100] The starting provision would be an obligation to provide consumers with information about the collection and commercial exploitation of their data for analytical purposes.[101] An update to the Unfair Contract Terms Directive – foreseen for the new Commission regulation period 2019-2024 could include provisions on fair use of data. At the high level, the Unfair Contract Terms Directive introduced the notion of "good faith" to prevent imbalances in the rights and obligations

[97] For instance, they should provide a statement of reasons each time they decide to suspend or terminate the use of their services by a business user.

[98] And there is a current trend, see the Commission/Facebook Press Release 2019. The explanatory note in the Online Intermediary Services Regulation mentions that the main goal of the regulation is to establish a legal framework that guarantees, in the first instance, transparent terms and conditions for business (and private it seems) users of online intermediation services. Business users are then also guaranteed, within this framework, effective possibilities for redress when these terms and conditions are not respected.

[99] 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 (Consumer Rights Directive), 2011/83/EU; see also the commentary in *Concise European Data Protection, E-Commerce and IT Law*, S. Gijrath, S. van der Hof, A.R. Lodder, G-J Zwenne, eds., 3rd edition, Kluwer Law International, Alphen aan de Rijn, 2018.

[100] 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 (Unfair Commercial Practices Directive), OJ 2005, L. 149.

[101] See also art. 6 Unfair Commercial Practices Directive.

of consumers on the one hand and sellers and suppliers on the other hand.[102] Besides, the Unfair Contract Terms Directive includes the blue list with an overview of terms that could be considered unreasonable.[103] These terms could be enhanced to include better terms on the (re-) use of a private user's data, including transfer thereof as well on transparency in terms of how there are treated in the context, for instance, of 'free services'.[104] The digital platform provider would have to make it clear from the beginning that the free of charge services require the use of data of the private user as a counter-performance.

What would be the consequence of non-transparent or incomplete contract terms on data use, and transfer? Such unfair contract terms are not binding for consumers. Moreover, the Directive also requires contract terms to be drafted in plain and intelligible language. As a consequence, ambiguities would be interpreted always in favor of consumers. This obligation could serve as a lever against opaque, incomplete or misleading provisions on the commercial exploitation of a private user's (personal) data, whether they represent a value or not. Misleading or false information, as in the CA case, would be considered an unfair commercial practice and should lead to sanctions.

Consumer law protection provisions could function as a meaningful instrument to empower the private users in contracts with digital platform providers. Some detail is necessary. A DTA should begin with specifying the scope of the property rights in data attached to the transfer and the purposes for the transfer.[105] But, as was demonstrated above, such a qualification requires prior legal analysis as to what data input must be provided to the data analytics company.[106] Let me remind the reader of the problems with scoping property in data transfer agreements when there is no nexus between the

[102] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts as amended, *OJ L 95, 21.4.1993, p. 29–34.*
[103] Terms Referred to in Article 3 (3) of the Unfair Contract Terms Directive.
[104] *Cf*. A. Metzger, "Data as counter-performance: what rights and duties do parties have?". 8 Journal of Intellectual Property, Information Technology and E-Commerce Law (2017), p. 2-8 (Metzger 2017). See also, more extensively: N. Helberger, F. Zuiderveen Borgesius, A. Reyna 2017, p. 1442-1449.
[105] This Paper does not deal with possible data license agreements, based on copyright or database rights in the source data. If have explained above that I am not convinced that an intellectual property rights approach to data will be functional. For an extensive discussion of IP rights in the source data and their implementation in a form of license agreement: B. Van Asbroeck, J. Debussche, J. César 2017-1, p. 59-78 on copyright and p. 82-105 on the exploitation of *sui generis* rights in databases.
[106] This would be an exercise similar to a privacy impact assessment.

private user and the third party.[107] Private law incorporates the notion of third party beneficiary rights. That would entail that the transferor should require from the transferee to include provisions in the DTA or in the contract with the digital platform provider to protect the personal data of the data subjects and that it should commit to certain contractual standards. This could be difficult to achieve, especially since the data subjects – often consumers, who sometimes are willing to grant access to their personal data in exchange of information or a price discount – have no standing in the negotiations.[108] Enforcing contractual accountability arrangements may prove to be difficult where the third party employs subcontractors or other third parties and fails to secure adequate obligations from those parties.

Finally, does the fact that the data subjects have little say on the transfer of – depersonalized personal data imply that there is a (stronger) duty of care on the third party to safeguard the data? An option that the Commission considers is issuing model contract terms, codes of conduct and/or default contract rules; along with a right to access for "public interest" and scientific purposes. It certainly does not appear impossible or impractical to further investigate how a DTA can impose both contractual and regulatory requirements; it just requires an open mind as to how to align personal data protection with private law to achieve a better result. It might engage data subjects more in the potential use risks *and* opportunities of big data analytics. Defining ownership rights and scoping in DTA's may also make the enforcement of competition law better manageable. The competition authorities will have a sound basis to start their investigation on.[109]

3.5 Interim conclusion

In sum, notwithstanding a number of pitfalls, a functional approach to consumer law and data protection is likely to yield better results for private users in terms of controlling

[107] B. Van Asbroeck, J. Debussche, J. César 2017-1, p. 5, conclude that "(…) such situation is not sustainable in a data-driven economy and with the fast-increasing development and adoption of data mining and analysis tools."
[108] General terms and conditions are as little negotiable as privacy policies. But if the FCO Ruling stands in appeal, that could entail a meaningful improvement to the private users' legal positions See, *infra,* para. 1.1.
[109] I will not discuss these same characteristics as an argument against having well written and detailed DTAs.

and monitoring what happens with the (non-personal and personal) data they hand over to the digital platform, consciously or not.

3.6 (Extra-contractual)liability for data (mis-)use?

An extra strong case for aligning private law with personal data regulation is the need to provide for liability for damages resulting from illegitimate data publishing and/or data loss or mutilation. If the legal qualification for data is complex and has not been fruitful in defining the rights and obligations of the parties involved both under property and contracts law, then what can be said about prospective contractual – or extra-contractual – liability?

First, it would be helpful to determine in the DTA what damage causing events could occur, when a party who either 'owns' or transfers the data to a third party. Examples of damages occurring in the big data analytics processes could be: (1) lost, destroyed, mutilated, garbled or otherwise damaged data, (2) manipulated, modified, abused or falsified data, (3) further transferred, (re-)sold data, or (4) published and made available data without consent.

Second, before addressing which party would be liable, the damage causing events need to be tied to actors.

Third, it is not sufficient to rely on general legislation regarding extra-contractual liability, for instance, risk liability. This requires a whole separate legal analysis of the law and the differences on liability legislation across the EU.

There is an instance where the EU already brought together a breach of community law and private law damage claims: the 2014 Directive on damages.[110] There are some fairly clear legal provisions in the GDPR on liability for damages suffered as a result of misuse of personal data. This "*Schutznorm*" may support private parties' claims. Article 82 GDPR provides that any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation.[111] This

[110] 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.

[111] A processor shall be liable for the damage caused by processing *only* where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. See also sections 3 and 4 of Article 82 GDPR. Section 3 provides that a controller or processor may exempt itself from liability if it proves that it is not in any way

norm could be applied to the third parties who provide big data analytics services. The wording in the GDPR is broad and concrete for data controllers and data processors to include liability provisions in their processing and big data analytics agreements. Recital (146) to the GDPR speaks for itself (emphasis added):

> "(…) *Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation."*

Second, the rights of the data subjects are set out:

> *"Data subjects should receive full and effective compensation for the damage they have suffered."*

Article 28, subsection 4 GDPR bears particular relevance for a digital platform service provider who enters into a big data analytics contracts with a third party. It actually provides a duty to contract in a straightforward manner (emphasis added):

> "*Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations*."

The consideration cited above should be translated into liability for misuse of personal data by controllers and processors alike. And the limitation of liability clause should be reasonable and compliant with the terms of the GDPR. I hope this section offers support to liability being an area where regulation and private law agreements should come together.

responsible for the event giving rise to the damage. Section 4 is the well-known provision establishing joint liability.

4. BIG DATA ANALYTICS AGREEMENTS: FOLLOW-UP?

Let us briefly return to the CA/Facebook controversy. It is not certain whether the transfer of data was supported by an agreement between CA/Facebook. Various regulatory authorities have investigated whether Facebook complied with its regulatory obligations and, at a more general level, whether it exercised a duty of care against CA. If they had, then this would entail that trust between the digital platforms provider and its users could be established. A contractual assessment of the scope of the contractual relationship between Facebook and CA brings a host of questions, such as:

(1) How was big data ownership qualified in the DTA?
(2) Did Facebook in fact provide CA with "non-personally identifiable information" only; were personal data masked adequately?[112]
(3) What did the parties agree on the scope, depth, performance, veracity and control of the output (big data) of the data analytics – did Facebook have a say?
(4) Did Facebook negotiate and have right to control whether big data analysis on non-personal data was performed and was compliant with privacy regulation?
(5) What did the DTA provide on contractual liability of either party under the DTA? Did the DTA contain an indemnification from CA to Facebook?

These questions serve to underline that it is preferred to have a DTA than to rely on data protection or competition law enquiries that reveal that the transferor has not exercise due care from the start of the transaction. Digital platforms' regulation could then supplement the contract by requiring the digital platform service provider that wishes to enter into DTA's with third parties to contract in user rights. Additionally, regulation could oblige the transferor to safeguard third party beneficiary rights on behalf of the data subject against the transferee.[113]

[112] See above under "Just another data policy."
[113] The EDPS considers that data portability helps competition and consumer protection, EDPS 2015, p. 13*ff*.

5. FINAL REMARKS

5.1 Let's not forget the stakeholders

The stakeholders should recognize the gap that exists between: (1) extensive personal data protection regulation and competition law and (2) the lack of (harmonisation of) legislation and regulation that provides for qualification of data and their collection under private law, including their use under unfair contract terms legislation. This justifies a functional approach to the applicable regulation. Even in a restricted property regime, the preference should be to specifically grant a property right to personal information in private law, simply because this is likely to enhance both their economic use and provide for the contractual enforcement of rights by the private users who see their data being processed outside their scope of control. In case personal information is recognized as a property right, then the legislation should provide the criteria for determining who owns the data.

If society wants private users to have the option to claim damages for misuse of their personal or aggregated data, then a nexus must be established with private law. Contractual arrangements regarding the onus of liability under any DTA may be subjected to scrutiny by NRA's or courts, when there is a serious breach of privacy rights of the data subject.[114] Only civil courts are competent to determine the basis for, the scope and amount of damages suffered by a data subject.

5.2 Back to the economic and trust factors

In this Article it was argued that the data economy and the digital platforms policies by themselves are inadequate to regulate behaviour of parties who make money from analysing human behaviour. The point was made that the digital platform provider is the man in the middle. It is really up to the platform provider to engage in setting the boundaries (the purpose limitation) with the data analytics company; and to survey contractual compliance.

If data are a resource, a commodity of their own, then affected parties are entitled to transparency on the transactions contemplated with the data they provided to the digital platforms. The private users have nothing to do with the third parties who perform big data analytics.

[114] See again the GDPR, recital (146) on conflicting court rulings.

The Commission and other EU institutions are uncertain that the market for the trade in for personal information is transparent, fair and efficient. Contracts could alleviate these concerns.

'Sharing' data – as it were – in exchange of 'free services' is not desirable if the private user does not have a clear understanding what the data might be used for; and how much value is attached to big data output.[115]

BIBLIOGRAPHY

[1] G.S. Alexander, E.M. Peñalver, *An Introduction to Property Theory,* Cambridge: Cambridge University Press 2012 (G.S. Alexander, E.M. Peñalver 2012).

[2] J. B. Baron, "Property as Control: The Case of Information", 18 *Mich. Telecomm. Tech. L. Rev*. 367 (2012) (J.B. Baron 2012).

[3] L. Bennet Moses, "How to Think about Law, Regulation and Technology, Problems with "Technology as a Regulatory Target", *Paper* http://dx.doi.org/10.5235/ 17579961.5.1.1. (L. Bennet Moses, 2013).

[4] M. Burri, M. Elsig, R. Polanco, R.Schär, S. Klotz, The Governance of Big Data in Trade Agreements: Design, Diffusion and Implications, work progress, University of Lucerne.

[5] M. Burri, "The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation", *UC Davis Law Review*, Vol. 51, 2017, pp. 65-133 (M. Burri, 2017).

[6] G. Calabresi, D. Melamed, "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral", 85 *Harv L. Rev.* 1089 (1972).

[7] D. Geradin, "Ensuring sound regulatory processes: For a principled approach", *TILEC Dicussion Paper DP 2017-030*, ISSN 1572-4042 (D. Geradin, 2017).

[8] European Parliament, *Report*, "Legislative Train", 06.2017 (European Parliament 2017).

[9] I. Graef, M. Husovic, "Response to the Public Consultation on 'Building a European Data Economy', *TILEC Discussion Paper, DP 2017-016*, ISS 1572-4042, April 2017 (I. Graef, M. Husovic, 2017).

[115] EDSP 2015, p. 12.

[10] I. Graef, M. Husovic, N. Purtova, “Data Portability and Data Control Lessons for an Emerging Concept in EU Law”, *Tilburg Law School Legal Studies Research Paper Series*, No. 22/2017 (I. Graef, M. Husovic, N. Purtova 2017).

[11] M. Granieri, A. Renda, *Innovation Law and Policy in the European Union, Towards Horizon 2020*, Springer, 2012 (M. Granieri, A. Renda, 2012).

[12] W. McGeveran, “Big data and privacy: making ends meet”, Conference Paper, 2012 W. McGeveran 2012).

[13]A. Metzger, “Data as counter-performance: what rights and duties do parties have?”. 8 Journal of Intellectual Property, Information Technology and E-Commerce Law (2017), p. 2-8 (Metzger 2017).

[14] M. Mourby, E. Mackey, M. Elliot et al., “Are ‘pseudonymised’ data always personal data? Implications of the GDPR for administrative data research in the UK”, *Computer Law and Security Review*, Volume 34, Issue 2, April 2018, Pages 222-233.

[15] N. Helberger, F. Zuiderveen Borgesius and A. Reyna, “The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law”, *Common Market Law Review* 54: 1427-1466, Kluwer Law International, 2017 (Helberger, Zuiderveen Borgesius, Reyna, 2017).

[16] McKinsey Global Institute, Disruptive technologies: Advances that will transform life, business and the global economy, paper, May 2013 (McKinsey 2013).

[17] J. Modrall, “Big Data and Algorithms, focusing the discussion”, Oxford University, Business Law Blog, 15 January 2018 (J. Modrall 2018).

[18] OECD, *Big data: Bringing competition policy to the digital era*, 2016.

[19] J. Prufer, C. Schottmüller, “Competing with Big Data” (February 16, 2017). Tilburg Law School Research Paper No. 06/2017; TILEC Discussion Paper No. 2017-006; CentER Discussion Paper 2017-007, https://ssrn.com/abstract=2918726 (J. Prufer, C. Schottmüller, 2017).

[20] N. Purtova, *Property rights in personal data*: *a European Perspective*, thesis, University of Tilburg 2011 (N. Purtova, 2011).

[21] PWC, “Benefiting from big data, A new approach for the Telecom Industry”, *Report* 2013.

[22] K. Radha, B. Thirumala Rao, Shaik Masthan Babu, K. Thirupathi Rao, V. Krishna Reddy, P. Saikiran, “Service level agreements in cloud computing and big data”, *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 5, No. 1, February 2015, pp. 158~165.

[23] C. Rees, “Who Owns Our Data?” (2014) 30(1) Computer Law & Security Review 75 (C. Rees 2014).

[24] B. Schermer, “Privacy and property: do you really own your personal data?” *Weblog*, Leiden University, 15 September 2015.

[25] E. Sherko, “Linguistic Transparency and Opacity in Compounding,” *Acad. J. Interdiscip. Stud.*, vol. 4, no. 3, pp. 590–593, 2015.

[26] E. Tjong Tjin Tai, “Data and the law of property”, WPNR: Weekblad voor Privaatrecht, Notariaat en Registatie [in Dutch], 149 (7085), 2015, 993-998 (Tjong Tjin Tai 2015).

[27] E. Tjong Tjin Tai, “Data ownership and consumer protection,” *Tilburg Private Law Working Paper Series*, No. 09/2017.

[28] TNO, Ecorys, IVIR, *Digital Platforms: an analytical framework for identifying and evaluating policy options*, Report, Ministry of Economic Affairs, the Netherlands, 2015.

[29] B. Van Asbroeck, J. Debussche, J. César, “Building the European Data Economy, Data Ownership, A new EU right in data”, *White Paper*, Bird & Bird, 1 January 2017 (B. Van Asbroeck, J. Debussche, J. César, 2017-1).

[30] B. Van Asbroeck, J. Debussche, J. César, “Data Ownership, A new EU right in data”, *Supplementary Paper*, Bird & Bird, 31 March 2017 (B. Van Asbroeck, J. Debussche, J. César, 2017-2).

[31] B. van der Sloot, S. van Schendel, “Ten Questions for Future Regulation of Big Data, A Comparative and Empirical Legal Study”, 7 (2016) JIPITEC 110 par.1. (B. van der Sloot, S. van Schendel, 2016).

[32] H.U. Vrabec, Uncontrollable Data Subject Rights and the Data-driven Economy, dissertation, University Leiden, 2019 (Vrabec 2019).