Legal Barriers and Enablers to Big Data Reuse

A critical assessment of the challenges for the EU law

Helena Ursic[1], Bart Custers[2]*

Abstract: Extracting the value from big data assets is one of the goals the European Commission set in the Europe 2020 Initiative. However, a number of influential voices from the academia as well as from the practice have been suggesting that the current European regulation may not adequately address the challenges of big data. This paper aims to identify existing legal barriers and enablers to big data reuse in the EU law based on the approach that follows the traditional dichotomy of laws. In the public law part we analyse data protection law, privacy law and human rights provisions, data retention law, data localisation law and cybersecurity law. On the private law side the relevant areas are intellectual property rights law, competition law and consumer protection law. We find that the EU regulatory landscape is highly complex when it comes to data reuse. Claiming that as a general proposition the EU law should be labelled as a barrier or as an enabler does not hold much water. Nevertheless, the most important barriers and enables are identified, which may be useful for further regulating data reuse in order to facilitate a sustainable and dynamic digital environment.

Keywords: European Union, Big Data, Data Reuse, Legal Framework, Barriers, Enablers

I. Introduction

Despite of its buzzword status and wide usage in a variety of contexts, big data still has no well-established definition. Most often, it is characterized by the *variety* of sources of data, the *velocity* at which they are collected and stored, and their sheer *volume*, commonly known as the "3-V definition".[3] It is not clear which size datasets need to have, to label it big data, but big data obviously deals with many terabytes and petabytes.[4] The burning question, however, does not regard the definition of big data, but is how big data can create value, what its economic benefits are and how it can help the leading companies outperform their peers.[5] Some of the world's most successful and innovative companies such as Google, Facebook, Amazon, and eBay have built their business model on the collection and exploitation of big data.[6] In a similar way that oil laid the foundation of the smokestack economy, big data is believed to become the lifeblood of the

[1] Helena Ursic LLM is researcher at eLaw, the Centre for Law in the Information Society at the Faculty of Law of Leiden University, the Netherlands.
[2] Bart Custers PhD MSc LLM is research manager at eLaw, the Centre for Law in the Information Society at the Faculty of Law of Leiden University, the Netherlands, and head of the research division on Crime, Law Enforcement and Sanctions of the research center (WODC) of the Ministry of Security and Justice, the Netherlands.
[3] Douh Laney, *3D data management: controlling data volume, velocity and variety* (Stamford CR: Meta Group Inc. 2001).
[4] Amir Gandomi and Murtaza Haider 'Beyond the hype: Big Data concepts, methods and analytics' (2015) 35 *International Journal of Information Management* 2, pp. 137-144.
[5] McKinsey Global Institute, *Big data: The next frontier for innovation, competition, and productivity* (2011).
[6] These companies are listed as the world's largest corporations on the Fortune 500 list for 2015 <http://fortune.com/fortune500/>.

information economy.[7] It therefore comes as no surprise that extracting the value from data assets is one of the goals the European Commission (EC) set in the Europe 2020 Initiative.[8] Value creation through big data reuse is seen as a big potential and a not-to-be-missed opportunity for the EU.

The emergence of big data and its proven benefits have added to the complexity of the legal discussion, since the current regulation may not sufficiently respond to the challenges related to big data sets.[9] On the one hand, there have been claims that our society should expect a substantial loss of benefits of big data, if it attempts to confine it within an obsolete legal framework.[10] On the other hand, we cannot turn a blind eye on the grey side of big data revolution and its numerous risks.[11] Big data *reuse* in particular is a complex and blurred legal concept that could be an increasing source of consumer detriment in terms of privacy, security and consumers' rights.[12]

In the EU law, *reuse* is defined in Article 2 of *The Directive 2003/98/EC on the re-use of public sector information* (PSI Directive) as the use by persons or legal entities of documents held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced.[13] Hence the scope of the PSI is on documents rather than on data. This definition only applies to public sector information and does not necessarily fit the private domain.

Apart from the abovementioned provision, there has been no other European-wide definition of data reuse adopted yet. To understand the concept, we thus had to look at some other sources. Schneier defines data reuse simply as secondary use of data that follows initial collection and use. [14] However, even when this distinction is used for defining data reuse, it can be useful to split data reuse into more subcategories. For instance, an important legal distinction is whether data is reuse within the original purpose or beyond the original purpose (which is likely to constitute function creep). Another important distinction is whether the data is reused within its original context. Whether there is data repurposing and/or data recontextualisation depends on how and for which purposes the data is reused and on the conditions under which the data was originally collected.[15]

Our paper has no ambition to provide a final definition of data reuse. Rather, data reuse is considered in open terms as an analytical framework for the legal analysis and includes any type of secondary use of data.

---

[7] Dennis D Hirsch, 'The Glass House Effect: Big Data, the New Oil, and the Power of Analogy' (2014) 66 Me. L. Rev. 390.
[8] Commission (EC), 'Towards a Thriving Data Driven Economy' (Communication) COM (2014) 442 final, 2 July 2014.
[9] Ira Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 International Data Privacy Law 74. See also Tal Z Zarsky, 'The privacy-innovation conundrum' (2015) 19 Lewis and Clark Law Review 1, p. 160.
[10] ICO, 'Big data and data protection', 20140728, Version: 1.0. For further discussion also see Omar Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 11 Northwestern Journal of Law and Policy 5, pp. 239-273; Christopher Kuner et al., 'The challenge of ''big data'' for data protection' (2012) 2 International Data Privacy Law 2, pp. 47-49.
[11] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (New York: Houghton Mifflin Harcout, 2013).
[12] David Currie, 'The new Competition and Markets Authority: how will it promote competition?' (2013) The Beesley Lectures <https://www.gov.uk/government/speeches/the-new-competition-and-markets-authority-how-will-it-promote-competition>.
[13] A consolidated version of the directive <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:02003L0098-20130717>.
[14] Bruce Schneier, 'Risks of data reuse' (*Schneier on Security*, 28 June 2007) <https://www.schneier.com/blog/archives/2007/06/risks_of_data_r.html>.
[15] Bart HM Custers and Helena Ursic, 'Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection' (2016) 6 International Data Privacy Law 1, pp. 1-12.

Whereas other papers often address big data issues from particular legal perspectives, such as data protection law or intellectual property law, the main purpose of this paper is to provide a more general overview of the entire EU legal framework for big data reuse and to identify the requirements that influence data reuse activities. The key outcome will be a high-level analysis of critical areas discussing a number of existing legal barriers and enablers. This analysis can serve the legal audience well as an overview of the complex regulatory landscape for data reuse for. Moreover, the identification of the most important barriers and enables may be useful for law-makers and policy-makers for further regulating data reuse in order to facilitate a sustainable and dynamic digital environment.

In order to structure the analysis we distinguish two realms, private law and public law, following the traditional dichotomy of laws.[16] Law that regulates the vertical relationship between the state and private parties shall be deemed public whereas law that applies to horizontal dealings among private parties shall be labelled private.[17] Among the legal areas that prove relevant for data reuse, data protection law, intellectual property law and competition regulation are clearly in the front line, but, as will be shown, also other areas of law may be applicable to some extent.

The selection of the areas of public law is limited to: data protection law[18], privacy law and other human rights, data retention law, data localisation law and cybersecurity law. The selection of areas of private law is limited to: IPRs law, competition law and consumer protection law. We have acknowledged the EU's endeavours in regulating data reuse in the public domain, which have been an indispensable part of the legal discussion on open data in Europe since early 2000s.[19] In the private sector, however, considerably little and mostly partial analysis on data reuse has been performed yet, in spite of the EC's appeal to understand open data in a broader sense, i.e., including the private sector's initiatives.[20] To fill that gap, this paper also focuses on the regulatory landscape for the private sector.

Our contribution describes the first results of the EUDECO project,[21] an EU funded project under the Research and Innovation Framework Program Horizon 2020 of the European Commission. In this 3-year project, 6 partners from 5 countries work together on modelling the European data economy (EuDEco).[22] The EuDEco project is focused on addressing the question of reusing data from economic, technological, social/ethical and legal perspectives.

[16] Jaap Hage and Bram Akkermans, *Introduction to Law* (Springer International Publishing, 2014), p. 38.
[17] Michel Rosenfeld, 'Rethinking the boundaries between public law and private law for the twenty first century: An introduction' (2013) 11 International Journal of Constitutional Law 1, p. 126.
[18] Data protection law straddles the boundaries between public and private law, criminal and civil law. This makes it difficult to firmly place data protection law within any one of the legal categories traditionally employed by the doctrines of private international law. See for example Lee A Bygrave, 'Determining Applicable Law pursuant to European Data Protection Legislation' (2000) Computer Law & Security Report 16, pp. 252–257. Given the stronger human rights foundation that data protection law enjoys in the EU, in this paper we deliberately classify it under the realm of public law.
[19] DIRECTIVE 2003/98/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the re-use of public sector information [2003] OJ L 345. See also LAPSI, The European Thematic Network on Legal Aspects of Public Sector Information <http://lapsi-project.eu.halotest.cc.kuleuven.be/about-lapsi-20>.
[20] Giuseppe Abbamonte, Keynote speech at the European data forum, 16-17 November 2015, Luxembourg.
[21] EuDEco project <www.data-reuse.eu>.
[22] Grant Agreement No. 645244.

This paper is structured as follows. Section II describes the notion of data reuse. Section III explains the approach we took to position data reuse within legal borders. Section IV and V assesses data reuse from the perspectives of the selected legal areas. Section VI provides conclusions.

II. Public law overview

1. Data protection rules

Since a considerable and often the most valuable part of reused information relates to individual persons,[23] personal data protection rules are highly significant for data reuse. It is thus sensible to begin with a short overview of data protection law. *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (DPD)[24] adopted in 1995 has remained the fundamental European legal act in the area of data protection until today. The directive applies to processing of personal data, which means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (Article 2(b) of the DPD). Although not mentioned explicitly, data reuse can be seen as part of the broadly defined processing activities. The scope of the directive is delineated in Article 2 (a) by defining personal data as any information relating to an identified or identifiable natural person ('data subject'), who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. The core provisions of the DPD are found in Article 6, and are commonly referred to as privacy principles.

Due to the limited space, our short analysis of data protection law will only address three privacy principles that seem directly relevant to data reuse. We will base the analysis on the current version of the EU data protection law set forth in the DPD, but we will also make some references to the proposed General Data Protection Regulation (GDPR)[25].

The initial and critical point of every data processing is its lawfulness (Article 6(a)), which in turn means that a valid legal basis must be secured before each processing. The DPD recognizes the following five bases (Article 7):

(a) the data subject's unambiguous consent;

(b) processing is necessary for the performance of a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject;

[23] Anna Bernasek, *All you can pay* (Nation books New York, 2015), p. 328.
[24] [1995] OJ L 281.
[25] Position of the Council at first reading with a view to the adoption of a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2012/0011 (COD), Brussels, 6 April 2016.

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

In cases of data reuse, many of the legal bases above will hardly be used in practice. For instance, it is difficult to imagine how data reuse could be a requirement to perform a contract (b). As Article 29 Working party (WP) notices, Article 7(b) must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract.[26] For example, the provision will not be a suitable legal ground for building a profile of the user's tastes and lifestyle choices based on his clickstream on a website and the items purchased. This is because the data controller has not been contracted to carry out profiling, but rather to deliver particular goods and services.[27]

Also, it is very unlikely that invoking a data subject's vital interest (d) or a general public interest (e) would legitimate data reuse. Both provisions suggest that they have a limited application. First, the phrase 'vital interest' appears to limit the application of this ground to questions of life and death. Second, the 'general public interest' refers to public tasks that are assigned to an official authority or that are imposed on a private part by a public body.[28]

Thus, consent (a) or a data controller's legitimate interest (f) will probably be used as a legal basis. But even then, it will not always be easy for a commercial reuser to justify the processing. A valid secondary consent is difficult to receive, especially if some time has passed since the initial consent was gained. A legitimate interest of a commercial performer, probably closely related to its business goals, will suffice if it outweighs the importance of the right to data protection. As stressed by the researchers involved in the LAPSI project, data protection is considered a fundamental right; hence a data reuser might have a hard time proving that its interest wins over privacy.[29]

The WP takes a more balanced approach. It states that when interpreting the scope of Article 7(f), it is necessary to ensure the flexibility for data controllers for situations, where there is no undue impact on data subjects. However, it is important that data subjects are provided with sufficient legal certainty and guarantees, which prevents misuses of this open-ended provision.[30]

In addition to the notion of lawfulness, Article 6(a) also contains the principle of fairness, which is elaborated through the provision on the right to information in Article 10.[31] Data subjects have to be provided with information about the processing in an intelligible form including the details of: purposes of processing, the categories of data concerned, the data undergoing processing, the recipients or categories of recipients to whom the data are disclosed, any available information

[26] Article 29 Working Party 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (WP 217), p. 16.
[27] *Ibid.*, p. 17.
[28] *Ibid.*, pp. 20–21.
[29] LAPSI, (2012) Policy Recommendation N. 4 Privacy and Personal Data Protection <http://www.ivir.nl/publicaties/download/1098>.
[30] *Supra*, note 28, p. 10.
[31] Edoardo Ustaran et al., *European Privacy: Law and Practice for Data Protection Professionals* (International Association of Privacy Professionals, 2012), p. 106.

about the source and logic involved in any automatic processing of data. Data controllers usually provide this information in their privacy policies or in their terms and conditions, but these are not always easy to understand.[32]

In the context of data reuse, the fairness principle and the closely related right to information do not cease to apply. On the contrary, at this point it becomes even more important that the data subject is fully informed about the activities in which he is indirectly involved through his own data. There are two options how to ensure data subject's awareness. First, data reuse activities that might happen in the future are described and communicated to the data subject before his personal data is collected. Second, the data subject renews his consent every time before the data is reused for a new purpose, based on the information communicated through the updated privacy policy. Both tactics prove difficult to apply. In the first case, it is hard to predict all the purposes for data reuse that may arise in the future. In the second case, it is almost impossible to get in touch with all data subjects and to secure their valid consent.[33]

Conveying adequate information to an individual not only indicates fairness of processing, but it is an indispensable source of transparency and individual involvement. Only after receiving clear information the data subject is able to invoke his "core" rights such as right to access, erase and object.[34] Informing a data subject about data reuse, establishes the right balance between the right of the individual to have control over his or her data and the flexibility required for businesses to develop and innovate and make best use of the vast amount of data generated online and offline. As pointed out by the UK Information Commissioner's Office (ICO), the processing of big data can challenge the reasonable expectations of privacy that data subjects may have.[35] An example would be the purchase of data from a social media provider by a data broker. Absent clear information on data reuse, a user may not be aware how his data is shared nor may he expect such a trade.[36]

Finally, one of the most significant provisions for data reusers is the principle of purpose limitation and specification set forth in Article 6(b) of the DPD. It requires that the data is only used for a purpose compatible with the one for which it was collected.

Controllers have to determine the purpose of processing before the processing of data starts.[37] The chosen legal basis will only be valid for this specific purpose. For instance, consent will count as valid only for the cases of data use and reuse, which the controller communicated at the moment of the data collection.

The principle of purpose limitation is thus seen as an onerous, though a necessary barrier to excessive data use, profiling and analytics. Given the increasing prevalence of these practices, it has

[32] Bart Schermer, Bart MH Custers and Simone van der Hof, 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection' (2014) 6 Ethics and Information Technology, pp. 268-295.
[33] *Ibid*. The authors establish that privacy policies nowadays contain information overload, absent a meaningful choice for the users which leads to the situation where data subjects no more make informed decision but simply consent whenever they are asked to do so. Not only are data subjects unaware how their information and under what conditions will be processed, they also lack some basic understanding of whether their data can be and will be reused.
[34] Article 12 of the DPD.
[35] ICO, Big data and data protection 20140728 Version: 1.0 <https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf >.
[36] European Data Protection Supervisor, 'Opinion 7/2015, Meeting the challenges of big data - A call for transparency, user control, data protection by design and accountability' 19 November 2014.
[37] Article 29 Working Party 'Opinion 03/2013 on purpose limitation' (WP 203), p. 15.

been suggested that data protection strives more for regulating the decision-making stage than for regulating the data collection and data processing stages.[38]

Careful observance of the purpose limitation has been stressed by the European Data Protection Supervisor (EDPS) as one of the key decisions of accountable organizations. Also, the EDPS emphasized the importance of the context in which data is reused. Reusers have to consider whether data initially used in one context can be legitimately used in another context.[39]

In practice, it is unlikely that all possible reuses can be defined or predicted in advance. Admittedly, data reuse can be included in the purposes specified by the data controller by using a broad purpose formulation. Social networks' data use policies typically lacks specificity, both with regard to the data the networks collect as well as with regard to how they use this data. For instance, Facebook's privacy policy from 2015 only identifies categories of purposes by using vague descriptions such as "Provide, Improve and Develop Services"; "Promote Safety and Security"; "Show and Measure Ads and Services").[40] However, this can be seen as circumventing the intention of the legislator and processing based on it can be considered illegitimate.

The proposed regulation on data protection seems to shed some light in that direction. The Council's amendments have improved the provision on purpose limitation with a more detailed guidance for data reusers. In case of further processing the judgment on the compatibility of processing should be based on the following criteria: (a) links between the purposes for which the data have been collected and the purposes of the intended further processing; (b) the context in which the data have been collected; (c) the nature of the personal data; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards.[41] Another form of the compatibility assessment was proposed by Article 29 Working party in the Opinion on purpose limitation. The Party suggests a combination of a formal assessment, focused on the comparison between the purposes provided by the controller and actual data reuse and subjective assessment, focus on the context and the way the purposes can be understood, to determine the compatibility of data reuse.[42]

2. Privacy law and other human rights provisions

Data reusers increasingly seem to make use of aggregated, anonymized data. Anonymization is a process of turning data into a form, which does not allow the identification of an individual.[43] Non-identifiable data is no longer personal data; hence, data protection law does not apply anymore. Data reusers are particularly keen to adopt that technical solution when the legal regime for protection of personal data is considered too restrictive. Anonymized data can be as useful as personal data in many cases. A typical example may be a company that wants to personalize its marketing campaigns with the help of profiling. The use of personal data may be helpful to assess which people are potentially interested in particular products or services, but aggregated data on

[38] Bert-Jaap Koops, 'The trouble with European data protection law' (2014) 4 IDPL 4, pp. 250-261.
[39] *Supra,* note 37, p. 13.
[40] Brendan van Alsenoy et al., 'From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms' (2015) <https://www.law.kuleuven.be/icri/en/news/item/facebooks-revised-policies-and-terms-v1-2.pdf>.
[41] *Supra,* note 27 (Art.6, para. 4).
[42] *Supra,* note 37.
[43] ICO, Anonymisation: managing data protection risk, Code of practice, <https://ico.org.uk/media/1061/anonymisation-code.pdf>.

street level or neighbourhood level may be similarly useful and cheaper to process, as there are no consent procedures required and no detailed selection procedures necessary.[44]

Different degrees of anonymity exist. Anonymity exists when the identity of a data subject is not known and cannot be known. Pseudonymity exists when different transactions of one person can be linked to each other and to an specific entity without knowing the identity of this entity. An example may be a PIN code at an ATM: transactions can be related to the card, without knowing who made the actual transaction with the card. In line with the definition of personal data from Art. 2 of the DPD, data protection requirements also apply to pseudonymized data. Although Article 29 Working Party promotes pseudonymisation as a useful security tool, it emphasizes that by pseudonymisiation of data a data controller does not escape data protection requirements.[45]

Since it has become clear that it is not possible to establish with absolute certainty that an individual cannot be identified from a particular dataset of anonymized data in combination with other data that may exist elsewhere,[46] the EDPS has encouraged those who employ anonymization techniques to carefully use such techniques in combination with other safeguards. Anonymization cannot be achieved by just stripping a dataset of some directly identifying attributes but requires a much more prudent approach.[47]

In the absence of data protection law applicability, the EU law still grants some protection to data subjects. The protection of private life as guaranteed in Article 7of the EU Charter, which is not limited to situations involving the processing of personal data but also covers spatial, physical and relational privacy, as well as some other provisions on fundamental rights, can offer some legal safeguards.[48]

As indicated above, big data and its reuse may be useful for profiling purposes, but the results from profiling and other types of data analyses may turn out to be stigmatizing or discriminating. When selecting individuals or groups of people on particular characteristics, this may be unwanted or unjustified or both. Selecting for jobs, offering products and services to specific groups only, and some other decision-making is considered unethical and, in many countries, forbidden by (anti-discrimination) law when it takes place on the basis of gender, ethnic background, etc. When risk profiles constructed by companies, governments or researchers become 'public knowledge', this may also lead to stigmatization of particular groups. Discrimination and stigmatization on a large scale may also result in polarization of (different groups of) society.

Big data can even put pressure on human dignity. Solove[49] argues that in our information society, the reputation of people is more and more constituted by the data that is disclosed about them. Such disclosure of personal data can be voluntary or involuntary. As a result, people are also increasingly judged upon their digital representation (the digital person) rather than human beings of flesh and

[44] For more examples, see Tal Z Zarsky, ''Mine your own business!': Making the case for the implications of the data mining of personal information in the forum of public opinion' (2003) 5 Yale Journal of Law and Technology 1.
[45] Article 29 Working Party (2014), Opinion 05/2014 on Anonymisation Techniques, WP 216, p. 20.
[46] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2009) UCLA Law Review, 57, p. 1701.
[47] *Supra,* note 38, p. 5.
[48] *Supra,* note 45.
[49] Daniel J Solove, *The future of reputation: Gossip, rumor, and privacy on the internet* (New Haven Conn. u.a.: Yale Univ. Press, 2007).

blood. Practices like profiling can reinforce a tendency to regard persons as mere objects.[50] An example of a relationship based on digital reputation, trust and economic dependence is the sharing economy. According to a recent workshop at the FTC, the reputation could replace the regulation, if the sharing economy continues to grow in the future.[51] This may be particularly problematic when characteristics of digital identities are incorrect or incomplete or when automated decisions (i.e., without further human interference) are made upon individuals based solely on their digital identity.[52] A related issue is the so-called chilling effect, which refers to the fact that people may alter their behaviour when they are aware that they are being monitored. Sometimes, for instance in cases of camera surveillance, the aim is precisely to make people behave 'better', but a more general effect may be that people behave more modest and reluctant overall, reducing their freedom of expression and other important human rights and values.

Finally, data reuse can even challenge liberty and justice. The lack of privacy in the data economy greatly increases the possibility of price discrimination and influences some basic postulates of the free market.[53]

3. Data retention laws

Contrary to the areas discussed above, data retention laws present an example of a regulation, which rather encourages than restricts data reuse. Namely, its main purpose is to ensure there is sufficient amount of telecom data available to law enforcement for later reuse, under strict conditions. While fighting crime is no doubt a valid argument for data collection and reuse, the example shows how human rights can be at stake.[54] Moreover, the retention requirement imposes some significant administrative and financial burden to the communication providers, making it undesirable from the economic perspective.

In 2006, the European Union issued the Data Retention Directive.[55] This is perhaps the best known example of a data retention law. According to this directive, member states had to store the telecommunications data of citizens for a period of 6 to 24 months. Law enforcement agencies and security agencies were allowed to request a court access to the data for criminal investigations and prosecution. On April 8th 2014, however, the Court of Justice of the EU declared the directive invalid, because it violates fundamental rights.

Data retention laws described above should not be confused with data retention requirements, mostly non-binding or imposed as self-regulation, that are part of industry-specific laws, codes of conduct or private agreements. Those requirements should be interpreted in line with the EU data protection regulations and should comply with the principles of data protection law, in particular

[50] Lee A Bygrave, *Data protection law: Approaching its rationale, logic and limits*. *Information law series: Vol. 10* (The Hague: Kluwer Law International, 2002).
[51] Federal Trade Commission, 'The "Sharing" Economy: Issues Facing Platforms, Participants, and Regulators' <https://www.ftc.gov/system/files/documents/public_events/636241/sharing_economy_workshop_announcement.pdf>.
[52] Note that EU personal data protection law prohibits automated decision-making that is solely based on automated processing of data. See Article 15 of the DPD.
[53] *Supra,* note 25.
[54] Those serious surveillance concerns have in many states led to the revocations of data retention provisions, including the revocation of the EU Directive by the CJEU.
[55] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105.

with the principle on data quality and on lawful processing (Article 6 para. 1 (a),(b) of the DPD).[56] An example is the Code of Practice on Secondary Use of Medical Data in Scientific Research Projects, which provides that medical data is retained for a period of time that is needed to ensure reproducibility and verifiability of the findings.[57] For pseudonymized and anonymized data the conditions are more lenient. Similarly, search engines' providers follow the retention period as determined in their industry's best practices. In the EU, Article 29 Working Party has advised them to limit the retention of personal data (search terms) to 6 months.[58] In the world of increased data sharing, selling, licensing and other types of data reuse, data retention is desirable as it enables leveraging on the acquired data by performing indefinite data mining. Many commercial players will therefore be reluctant to delete the data they process and try to circumvent the legal provisions by drafting open and inexact data privacy policies.[59]

4. Data localisation laws

In the post-Snowden era, the idea of a transnational Internet where the information is freely moving cross-border has been challenged by a number of legislative proposals containing provisions on data localization. Those are data localization requirements, which refer to laws, or parts of laws, that limit the storage, movement and/or processing of data to specific geographies and jurisdictions or that limit the companies that can manage data based upon the company's nation of incorporation or principal sites of operations and management.[60] A striking number of countries have been moving closer to this paternalistic approach to cross-border data transfers by adopting various legislative measures with a common characteristic to encumber the cross-border data transfers.[61] A significant example of data localisation has been Russia with its amended draft law On Personal Data and On Information, Information Technologies and Protection of Information stating all personal data of Russians to be collected and recorded on the servers in Russia.[62] A number of other countries have also proposed data localisation laws: Australia, Brazil, Canada, China, Vietnam, South Korea, Kazakhstan, Taiwan and even some EU member states e.g. Germany and France.[63]

The motives are very diverse. At the top of the list are placed fear of foreign surveillance, followed closely by privacy and security concerns, endeavours for better law enforcement and development of national economies.[64]

By creating "Schengen zones for data" data localisation laws are undermining the possibility of global services as well as the major new advances in information technology.[65] The implications of these regulations on cloud computing, Internet of Things and big data, where cross-border flow of

[56] See DPD, Art. 6 (1)(a) and 6 (1)(d),(e). See also Alexander Tsesis, 'The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data', (2014) 49 Wake Forest L. Rev. 433.
[57] Article 7 <http://www.etriks.org/wp-content/uploads/2014/12/Code-of-Practice-on-Secondary-Use-of-Medical-Data-with-recognition.pdf>.
[58] Article 29 Working Party, Opinion 1/2008 on data protection issues related to search engines (No. WP148, 2008), p. 19.
[59] *Supra,* note 42.
[60] Jonah F. Hill, 'The Growth of Data Localisation Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders' (The Hague Institute for Global Justice, Conference on the Future of Cyber Governance, 2014).
[61] Anupam Chander & Uyen P Lê, 'Data nationalism' (2014) 64 Emory Law Journal 3.
[62] Anna Shashina, *'Update on amended Russian data protection legislation: news from the DPA conference in Moscow'* (*Bird&Bird,* 12 November 2014) <http://www.twobirds.com/en/news/articles/2014/global/update-on-amended-russian-data-protection-legislation-dpa>.
[63] *Supra,* note 61.
[64] *Ibidem.*
[65] *Supra,* note 62.

information and unlimited access to data is one of the main enablers, could be seen as a threat to the rising digital economy and effective (big) data reuse.

5. Cybersecurity law

The extent of data gathering, selling, and free dissemination of private derails, with few regulatory controls, opens many avenues for misuse.[66] For example, exploitation of big data through adversaries might open doors to new type of attack vectors.[67] The EU Commission plans to tackle some of these issues with a Network and Information Security (NIS) Directive, proposed in early 2013.[68] The draft directive aims to improve the security of the Internet and the private networks and information systems underpinning the functioning of our societies and economies.

The Commission acknowledges that the Data Protection Directive already contains a number of rules related to the security standards for controllers, including reusers, of personal data. However, there have been no rules relating to those that control, or reuse, non-personal data. For example, a network and information security breach affecting the provision of a service without compromising personal data (e.g. an ICT outage at a power company resulting in a blackout) would not have to be notified.[69] The NIS directive fills that gap by requiring market operators to notify critical breaches to national authorities and to ensure an adequate level of security for their information assets (Article 14, para. 1 and 2).

III. Private laws overview

1. Intellectual property law

Intellectual property rights (IPRs) protect immaterial goods, which are mostly the product of a creative mental human activity in the industrial, scientific, literary and artistic fields.[70] Among all the IPRs[71], copyrights, database rights and trade secrets are most closely related to data. Patents can apply to computer implemented processes that manipulate and process data, but generally not in relation to data itself.[72] Trademarks can apply to data products (like indices), but again, generally not in relation to the actual data.[73] In line with this view, our analysis will focus on copyrights, the *sui*

[66] Alexander Tsesis, 'The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data', 49 Wake Forest L. Rev. 433 (2014).
[67] ENISA, Threat Landscape Responding to the Evolving Threat Environment [Deliverable – 2012-09-28], p. 4 <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014>.
[68] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final, 7.2.2012.
[69] *Ibid.*, p. 6.
[70] Anette Kur and Thomas Dreier, *European intellectual property law: Text, cases and materials* (Cheltenham: Elgar, 2013), p. 2.
[71] The World Intellectual Property Organisation (WIPO) distinguishes six groups of intellectual property protection: copyrights and related rights, patents, trademarks, industrial designs and integrated circuits, geographical indications and protection against unfair competition, where trade secrets are of particular interest. For the classification also see Trevor Cook, *EU intellectual property law* (Oxford: Oxford Univ. Press, 2010).
[72] As patentability of software is not permitted under Article 52(2) of the European Patent Convention from 1973, the interference of patent rights on data reuse is limited. The dilemma of patentability of big data algorithms nevertheless remains arguable. See for instance Michael Mattioli, 'Disclosing Big Data' (2014). Articles by Maurer Faculty. Paper 1480.
[73] Richard Kemp, Legal Aspects of Managing Big Data (Kemp IT Law, 2014) <http://www.kempitlaw.com/wp-content/uploads/2014/10/Legal-Aspects-of-Big-Data-White-Paper-v2-1-October-2014.pdf>.

generis database right and trade secrets as it could be argued that these are the legal concepts that might influence data reuse activities in the EU most heavily, from an IPRs perspective.

Copyrights protect the form or expression of information but not the underlying information itself. They apply to software, certain databases, literary works, music, films, videos and broadcasts[74] that own a certain degree of *creativity* (also *originality*), which EU law defines as *'the author's own intellectual creation'*.[75] Copyrights arise automatically by operation of law in the EU (so that no registration is required) and constitute a formal remedy that stops unauthorized copying.[76]

Copyright is an important concern for data reusers. Any data analytics or data mining will often involve the wholesale copying of information or databases, many of which will be protected by IPRs in relevant jurisdictions.[77] Where data is not owned or licensed by the reusers, they will either need to find a viable exception to copyright or to abstain from data reuse.[78] However, it will not always be easy to determine who actually owns the data. The unambiguous ownership has been identified as a top-problem of open data use.[79]

In the EU, there have been some vocal observations suggesting the copyright laws should be transformed to better fit the needs of the digital society and data driven economy.[80] The EU Parliament has recently adopted a non-legislative report on copyright reform prepared by Pirate Party Member Julia Reda. The report calls for an adaptation of the EU 2001 Copyright Directive to the digital market and establishes the basis for the upcoming copyright reform proposal by the EU Commissioner for Digital Economy and Society.[81] In December 2015 the Commission published the communication "Towards a modern, more European copyright framework", in which it emphasizes the need for higher harmonisation and adaptation of copyright rules to new technological realities. Among others, the communication includes a proposal for a simplified cross-border access to online content services and the regulation of online platforms, in particular news aggregators.[82]

Another concept that can play an important role in data reuse is the legal protection of databases. Countries have addressed the issue in an uncoordinated fashion using diverse legal mechanisms

[74] Berne convention incorporates a longer non-exhaustive list of copyright protected works. The Berne Convention for the Protection of Literary and Artistic Works (Sept. 9, 1886).
[75] *Supra,* note 73, p. 252.
[76] David I. Bainbridge, Intellectual Property (Pearson Education, 2009), p.11.
[77] Richard Graham and Adam Lewington, *The Big Data Explosion: A New Frontier in Digital Law* (SCL – the IT law community) <http://www.scl.org/site.aspx?i=ed31114>. Also see Christian Handke, Lucie Guibault and Joan-Josep Vallbe, 'Is Europe falling behind in data mining? Copyright's impact on data mining in academic research' (May 20, 2015) http://ssrn.com/abstract=2608513>.
[78] RECODE, Legal and ethical issues in open access and data dissemination and preservation: Deliverable D3.1. (2014), p. 12. <http://recodeproject.eu/wp-content/uploads/2014/05/D3.1-legal-and-ethical-issues-FINAL.pdf>.
[79] In addition, mining of the social media content, which includes User Generated Content, created by a non-professional user without commercial purposes, can be legally challenging. Normally, the social networks would receive a user's approval to reuse his or her (IP protected) posts as part of the pre-registration consent to the standard terms of use. However, the researchers from KU Leuven have established that, at least according to Belgian legislation, such a blank approval does not suffice as a justification for IPRs reuse. *Supra,* note 55.
[80] See for example Primavera De Filippi and Katarzyna Gracz, 'Resolving the crisis of copyright law in the digital environment: reforming the "copy-right" into a "reuse right"' (2012) 7th International Conference on the interaction of knowledge rights, data protection and communication, Helsinki, Finland; Ian Hargreaves and Bernt Hugenholtz 'Copyright reform for growth and jobs' (2013) Lisbon Council Policy Brief, 13/2013.
[81] <https://juliareda.eu/copyright-evaluation-report/>.
[82] COM (2015) 626 final, 9 December 2015.

ranging from unfair competition rules to technological protection measures.[83] The European Union is an exception as it recognizes a unique right, exclusively aimed at the protection of databases, the so-called *sui generis* right, set forth by Directive 96/9/EC. The goal is to protect the content of databases that is not protected under copyright or data protection laws, but that amounts to a substantial investment, in time or money, for the collecting, verifying and presentation of the data (not the creation of the data themselves). Since its adoption by means of the Database directive, the *sui generis* right has received much criticism, including some negative feedback from the CJEU. Although the Court limited the scope of the data base right in its judgement in Case C-203/02 *The British Horseracing Board Ltd and Others v William Hill Organization Ltd*[84]*, sui generis* right is still considered a barrier to data reusers. Hargeaves and Hugenholtz claim the right is especially obstructing data mining and Big Data analytics.[85] Despite the critics, the database right is still fully applicable and data reusers should consider it carefully to avoid breaching IP law.

Contrary to the US federal legal system[86], there is no legislation on the EU level yet that would specifically concentrate on trade secrets.[87] Member states chose to regulate that area either in their commercial laws or through the prohibition of unfair competition. The protection of trade secrets often conflicts data reusers' goals, since it limits the access to datasets and reduce their exploitability.

2. Competition law

As a general proposition, competition law consists of rules that are intended to protect the process of competition in order to maximise consumer welfare.[88] Competition law is concerned with practices that are harmful to the competitive process, in particular with anti-competitive agreements, abusive behaviour by a monopolist or a dominant firm, mergers and public restrictions of competition.[89] Competition has gained central importance in the EU as one of the most powerful tools the authorities have to restore consumer's welfare.[90]

Competition law settles the conditions for a free and unrestricted access to market and this should also be the case on the market of (big, personal) data. National and EU competition authorities have over the last five or so years been showing increasing interest in analysing data through the lens of

[83] Estelle Derclaye, *The legal protection of databases: A comparative analysis* (Cheltenham, UK, Northampton, MA: Edward Elgar, 2008), p. 3.
[84] [2004] ECR II-2905
[85] Ian Hargreaves and Bernt Hugenholtz, 'Copyright reform for growth and jobs' (2013) Lisbon Council Policy Brief, 13/2013.
[86] In the United States, a federal source of law, the Uniform Trade Secrets Act, played a vital role in harmonizing the legal protection of trade secrets across the different U.S. states. In the EU this development has just begun. See for example Katarzyna A Czapracka, 'Antitrust and Trade Secrets: The U.S. and the EU Approach', (2007) 24 Santa Clara High Tech. L.J. 207.
[87] In November 2013, the European Commission proposed a draft directive that would align existing laws against the misappropriation of trade secrets across the EU.[87] A new framework for the protection of trade secretes was confirmed by the Council in 2014 and has been recently handed over to the Parliament to continue the regular legislative procedure.
[88] Richard Whish and David Bailey, *Competition law* (New York: Oxford University Press, 2012), p. 1.
[89] *Ibid.*, p. 3.
[90] *Ibid.*, p. 19. As ex-commissioner Neelie Kroes put it in her speech at the European Consumer and Competition Day in London in 2005, the EU competition law's aim is simple: *"To protect competition in the market as a means of enhancing consumer welfare and ensuring an efficient allocation of resources. An effects-based approach, grounded in solid economics, ensures that citizens enjoy the benefits of a competitive, dynamic market economy."* <http://europa.eu/rapid/press-release_SPEECH-05-512_en.htm>.

competition law in a number of sectors,[91] for example financial market data[92], geospatial data[93] and last but not least, personal data[94].

In the Google/DoubleClick case[95] the EC analysed whether the mere combination of DoubleClick's assets with Google's assets, in particular the databases that both companies have or could develop based on customer online behaviour, could allow the merged entity to achieve a position that could not be replicated by its competitors.[96]

The Commission also reviewed the case of a merger between TomTom/Tele Atlas.[97] The business goal of that merger was to enable TomTom re-using (integrating) and selling the information acquired from the new business partner Tele Atlas (the merged company).[98] Tomtom and TeleAtlas tried to defend the merger with an efficiency claim arguing that that data in the form of feedback from TomTom's large customer base would allow the merged firm to produce better maps faster.

In 2014 the European Data Protection Supervisor (EDPS) hosted a workshop to collect best practices and offered some guidance on possible interfaces between data protection law, consumer law and competition law.[99] The EDPS acknowledged that big data, which often contains personal information, plays the role of a currency for purchasing free services. For example, in the case of cross-sided platforms such as Facebook, data is easily (and freely) gained from the consumers on the one side of the market and then sold to advertisers on the other side.[100] If one of the players on that market acquires a dominant position, this might result in unwilling consequences such as tying, anticompetitive agreements or exploitation of competitors.[101]

The assessment of the merger between Facebook and WhatsApp, where the Commission checked whether post-merger Facebook would collect data from WhatsApp users (which are also Facebook users) and gain an advantage for targeted advertising, was, among others, concerned with the significance of personal data for the competition on the market. The Commission found no

[91] <https://research.bournemouth.ac.uk/wp-content/uploads/2014/02/BS-Borghi-Maurizio.pdf>.
[92] *Ibid*.
[93] Case COMP/M.4854, Commission Decision, C (2008) 1859.
[94] European Data Protection Supervisor, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy – preliminary opinion' (2014).
[95] Case COMP/M.4731, Commission Decision, C (2008) 927.
[96] Another aspect to be considered by the Commission in its investigation was the interaction between competition law and privacy. Interestingly, the Commission pointed out that it had referred 'exclusively' to the likelihood that the merger would impede effective competition in the common market. However, it noted that its decision was without prejudice to the merged entity's obligations under the Data Protection directive. Julia Brockhoff et al., 'Google/DoubleClick: The first test for the Commission's non- horizontal merger guidelines' (2008) Competition Policy Newsletter, pp. 59–60.
[97] *Supra,* note 95.
[98] TomTom integrates the navigable digital databases it purchases from Tele Atlas into the navigation software the company produces. The integrated product (software and database) is then either included in the portable navigation devices that TomTom itself sells to end-consumers or is sold to other manufacturers of navigation devices for inclusion in their devices.
[99] *Supra*, note 94.
[100] Damian Geradin and Monika Kuschewsky, 'Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue' (2013).
[101] EDPS considers the absence of a clear definition of a primary and a secondary data market a fundamental problem (see *supra,* note 94, p. 24). Namely, if there is no market definition, regulators cannot determine a dominant position or monopoly. Consequently, they have no basis to claim an abuse of dominance, which is one of the fundamental competition law breaches. Also, they would experience difficulties with proving anticompetitive agreements or mergers. The fact that online firms have been able to convince some (US based) courts that there is no product market for "free" services like search and convince agencies to treat online media as just another form of traditional media where the consumer can be ignored, paints a false picture. Maurice E Stucke and Allen P Grunes, 'Debunking the Myths Over Big Data and Antitrust' (2015) 5 CPI Antitrust Chronicle 2.

competition concerns even if Facebook would use WhatsApp as a new source of user data, as there remain a sufficient alternative providers of online advertising services with access to user data valuable for advertising purposes.[102]

When discussing if and how big data reuse should be subject to competition law, it is important that the authorities understand both the competitive benefits and risks of data-driven strategies.[103] Sometimes, a data-driven merger may provide sufficient scale for smaller rivals to effectively compete, however, at other times data may be used primarily as an entry barrier.[104] Both, the Google/DoubleClick case and the TomTom/TeleAtlas case were cleared. Nevertheless, the fact that the lengthy and costly assessment procedure was initiated confirmed the seriousness of the concentration and the likelihood of the negative impact to competitiveness in the EU. Also, there has been no investigation related to an abuse of a dominant position on the market of big data or personal data on the EU level so far, but, as the Commission puts it clearly, this cannot be ruled out.[105] The scenario, in which the finding of liability under Article 102 TFEU seems most likely, is where an access seeker needs the user data as an input for a new product that would not stand in direct competition to the main product that the online platform provider offers to its customers.[106]

3. Consumer protection

As the EU data protection supervisor (EDPS) made clear in his preliminary opinion,[107] consumer protection law plays a visible role in the data-driven economy in particular in ensuring transparency and accuracy of information. The EDPS predicts that the scope for abuse of market dominance and harm to the consumer through refusal of access to personal information and opaque or misleading privacy policies may justify a new concept of consumer harm for competition enforcement in digital economy.[108]

The UK regulator for markets and competition (CMA) has already embraced this position. In June 2015 it published a comprehensive opinion on commercial use of consumer data[109] listing a number of business practices that are arguably disputable under consumer protection law. For example, according to CMA misrepresenting the privacy, security, or confidentiality of users' information –

[102] Sophie Moonen, 'Competition law and data', European Commission, DG Competition, Head of Unit Mergers IT, Communications, Media GCLC – 14 September 2015 <https://webcache.googleusercontent.com/search?q=cache:cockGPmR8IkJ:https://www.coleurope.eu/sites/default/files/uploads/page/slides_sophie_moonen_0.ppt+&cd=1&hl=en&ct=clnk&gl=nl&client=safari>.

[103] Joshua D Wright et al., 'Comment of the global antitrust institute, George mason University School of Law, on the EC's public consultation on the regulatory environment for platforms', George Mason University Law and economics Research paper Series No 15-58, December 29, 2015.

[104] Maurice E Stucke and Allen P Grunes, 'Debunking the Myths Over Big Data and Antitrust' (2015) 5 CPI Antitrust Chronicle 2, p. 4.

[105] *Supra,* note 102.

[106] Inge Graef, Yuli Wahyuningtas and Peggy Valcke, 'Assessing data access issues in online platforms' (2015), Telecommunications policy 39, pp. 375–387.

[107] *Supra,* note 94.

[108] The European Commission shared a similar opinion in 2012: *"In the current economic context a strong consumer policy is a necessity. Empowering Europe's 500 million consumers will be a key contribution to growth in the European economy. The strategy adopted today aims to empower consumers and build their confidence by giving them the tools to participate actively in the market, to make it work for them, to exercise their power of choice and to have their rights properly enforced. We will do so* […] *by ensuring that consumer interests are more systematically integrated into EU policies of key economic importance for households."* (European Commission, 'A new European Consumer Agenda – Boosting confidence and growth by putting consumers at the heart of the Single Market' Press release, IP/12/491).

[109] Competition and Markets Authority, *The commercial use of consumer data, Report on the CMA's call for information* (CMA 38, June 2015).

which could still be deceptive, even if the privacy policy or other small print is factually correct (for example, the consumer is told that data is collected in order to complete a purchase) – violate the provision of fairness set down in the EU and UK national legislation.[110]

Big data reusers are bound to comply with data protection law, but in reality they often walk on the edge of law. The fact that their behaviour is regulated by both data protection and consumer protection rules could mean an additional safeguard for data subjects and hopefully more transparency in data reuse.

IV. Conclusions

Extracting the value from data assets is one of the goals the European Commission set in the Europe 2020 Initiative. However, a number of influential voices from the academia as well as from the practice have been suggesting that the current legal setting does not sufficiently respond to the challenges of big data. Based on the approach that follows the traditional dichotomy of laws we have identified existing legal barriers and enablers to big data reuse in the existing European legal framework. The analysis has shown the following: data protection law mostly acts as a barrier (aims at minimizing the amount of data that can be processed, prevents limitless retention, inflicts additional obligations on data reusers etc.). In rare cases data protection law can also act as an enabler, for example through the principle of data quality (an analysis of a more precise dataset would give more reliable results). Protection of human rights represents a barrier to data reuse, though a justifiable one. Human rights call data reuse into question when the latter is performed to follow the business objective regardless of the rights and interests of data subjects. Data localisation is an indirect barrier to data reuse. It deters international data transfers and therefore limits exchange and reuse of data on a global scale. By ensuring the data is available for additional analyses and examination in the future, data retention law acts as an enabler. Cybersecurity can be both, a barrier or an enabler to data reuse. If the requirements are too burdensome, then they deter processors from keeping the data and reusing it (barrier). However, by stimulating security those requirements can create a more trusted and secure environment that actually encourages data reuse (enabler). As regards the private law part, IPRs are barriers to data reuse when they limit data reusers to fully exploit datasets. They are enablers when they guarantee better legal protection and thus encourage authors to share their (IP protected) data. Competition law is a barrier when it limits a data owner that has a dominant position in the market. It is an enabler when it encourages fair competition. When data reusers reuse data to customize their marketing strategies and reach out to more clients, consumer protection law blocks those business conducts that are based on unfair practices (e.g. broadly defined purposes of data processing to enable easy contact with the costumers). On the other hand, data reuse can also be advantageous to consumers, when it (justly) helps achieve more precise and targeted advertising. In such cases consumer protection law takes a neutral position.

Based on the findings above we can conclude that the EU regulatory landscape is highly complex when it comes to data reuse. Claiming that as a general proposition the EU law should be labelled as

[110] Among others, CMA observes that (contrary to the Consumer rights directive (and implementing acts)) the Council directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts and its implementation act(s) applies whether or not the consumer pays with money – for example if the product is being provided in exchange for personal data. *Supra* note 109, p. 66.

a barrier or as an enabler does not hold much water. Nevertheless, identifying the most important barriers and enables for data reuse may be useful for further regulating data reuse in order to facilitate a sustainable and dynamic digital environment..[111]

[111] EDPS, Opinion 4/2015, Towards a new digital ethics, data dignity and technology, 11 September 2015 <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_EN.pdf>.