The value of personal data in a competitive information age

Does the Data Protection Regulation provide individuals sufficient control over their personal data or should competition law intervene?

Candidate number: 8011
Submission deadline: 15-05-2016
Number of words: 14808
Table of contents

Introduction ......................................................................................................................... 3
Methodology ......................................................................................................................... 4
Chapter 1  Who controls personal data online? ................................................................. 5
  1.1 The introduction of the Data Protection Regulation ...................................................... 6
  1.2 Personal information .................................................................................................... 7
      1.2.1 Sensitive personal data ....................................................................................... 8
  1.3 Controller vs processor ................................................................................................. 9
  1.4 Legal grounds for processing ..................................................................................... 9
      1.4.1 Consent ................................................................................................................ 10
      1.4.2 Legitimate interests ............................................................................................ 12
  1.5 Data protection principles .......................................................................................... 13
      1.5.1 Fair and legitimate processing ............................................................................ 14
      1.5.2 Principle of minimality ....................................................................................... 15
      1.5.3 Purpose limitation ............................................................................................. 16
Chapter 2  Extended rights for data subjects ................................................................... 18
  2.1 Data as property .......................................................................................................... 19
      2.1.1 Default rules ....................................................................................................... 19
      2.1.2 Inalienability of personal data ........................................................................... 20
      2.1.3 Remedies ........................................................................................................... 21
  2.3 Profiling ....................................................................................................................... 22
Chapter 3  Abusive nature of control over personal data ............................................... 23
  3.1 Privacy or competition ............................................................................................... 23
  3.2 Competition based on quality .................................................................................... 24
  3.3 Consumer welfare ....................................................................................................... 25
  3.4 Value of personal data ............................................................................................... 26
  3.4 Control over data ......................................................................................................... 26
  3.6 The rise of the ‘free’ .................................................................................................... 27
  3.7 Abuse of market power ............................................................................................... 27
      3.7.1 Lower privacy standards ..................................................................................... 28
      3.7.2 Price discrimination or other types of targeting ................................................. 30
      3.7.3 Data portability – the heart of competition law ................................................... 31
  3.8 New definition of consumer harm .............................................................................. 33
Conclusion ......................................................................................................................... 34
Table of reference ............................................................................................................. 37
Introduction

Personal information, as the ‘new currency of the digital world’, has a dual nature. Whereas on the one hand personal data can be considered to have monetary value, on the other hand it is intrinsically linked to privacy. The consideration of personal data as a ‘new currency’ stems from the enormous rise in volume of collected personal data and its use for commercial purposes. From massive piles of high volume (un)structured data (‘big data’) it is possible to extract exact data that can be linked to a specific individual. Such data is attractive to all sorts of advertisers and other companies online or offline. The rise of big data has posed questions related to this dual nature of personal data. This is evidenced by the acceptance of a new data protection regulation (the ‘Regulation’), which is supposed to give control over personal data back to the individuals. It can also be seen in debates about the role competition law to address privacy concerns on which I will provide more details later on.

The European Data Protection Supervisor (‘EDPS’) is also in favor of a stronger connection between the two fields of law. In March 2014 the EDPS published its Preliminary Opinion privacy and competitiveness in the age of big data (the ‘Report’). This Report reflects the interplay between data protection, competition and consumer law. According to the Commission big data introduces significant competitive advantages that could result in breaches of competition law. In anticipation of possible future synergies between data protection law and competition law, the German competition authority (‘Bundeskartellamt’) started an investigating on Facebook for suspected abuse of market power over breaches of data protection laws. Andreas Mund of the Bundeskartellamt said that ‘it is essential to also examine under the aspect of abuse of market power whether the consumers are sufficiently informed about the type and extent of data collected’. This investigation is the first time that

---

1 According to Meglena Kuneva, European Consumer Commissioner, March 2009 in SPEECH/09/156.
2 Brussels, 16 April 2016, Interinstitutional File 2012/0011 (COD), Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). The European Parliament approved the final text on 14 April 2016.
3 Recital 68 Regulation.
4 For instance, it has been debated on during privacy the European Parliament’s Privacy Platform on 21 January 2015 in Brussels and by Margareth Vestager in her speech about competition in a big data world of 17 January 2016.
5 Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data, March 2014 (hereinafter the ‘Report’).
6 The German Competition Authority.
7 See e.g. Reuters, ‘Germany takes on Facebook in competition probe’, 2 March 2016.
volume of personal data held by a company plays a significant factor in proving a breach of competition law.

This raises the question whether the Regulation provides sufficient control for individuals over their personal data, or whether competition law should in fact come out to play when privacy is concerned. I am of the opinion that competition law is not fit to encompass privacy analyses. This is acknowledged by Vestager, who focuses not so much on competition law but on having adequate data protection law to address a loss of control.\(^8\)

Therefore, I start off by addressing the question whether the Regulation, it’s main principles, are fit for the challenges of big data. These principles adhere to the idea that it is possible to decide on a certain processing purpose beforehand, while in fact, the added value of big data rests in the discovery of new correlations for new purposes. In the second chapter I will elaborate more on the Regulation and several newly introduced rights. While the principles of data protection mainly remain the same, it has been acknowledged that data subjects ought to be given more control. The Regulation includes strengthened rights that ensures this aim. Nonetheless, some people still think that competition enforcement action ought to be taken when the control of data by a limited number of undertakings, restricts others from being active on a certain market. In the third chapter I focus on how the use of personal data by undertakings can possibly breach EU competition law. In order to assess the impact of data on competition their economic properties must be regarded. At the end of these chapters I will conclude my thesis by answering the question whether the Regulation provides data subjects sufficient control over their data or whether competition law should be applied with privacy in mind to balance such lack of control.

**Methodology**

Please note that I focus on the processing of personal data for big data analytics. My opinion and ideas do not apply to all data processing. I should also note that my focus rests on the Regulation and not on the Data Protection Directive\(^9\) (‘Directive’) which will be effective for the coming two years. Since the Regulation has been approved by the European Parliament on 14 April 2016 it would seem a little redundant to discuss the current data protection

---

\(^8\) Speech by M. Vestager, see footnote 4.

framework. Furthermore, since my main focus is on data protection law, I will not go into in-depth analysis of competition law. My research is entirely literature-based. The evaluated resources will be limited to the Regulation (the final and the Council’s version), the Data Protection Directive, the Treaty of the Functioning of the European Union and case law of the ECJ and the European Commission. Secondary sources consist of books, journals, scholar papers, opinions and reports relevant to give weight to the discussion on this thesis’ topic.

Chapter 1 Who controls personal data online?

Over the last few years, the rise of the ‘information society’\(^\text{10}\) has enabled companies to collect huge amounts of data. Whereas the collection of data was an expansive and time-consuming activity in the past, it only takes a few seconds for modern day technologies to process non-structured data sets. Big data are high volume (un)structured data which can be mined to retrieve all sorts of information. According to the ‘Gartner’ definition, big data can be described in terms of the ‘three V’s’: volume, variety and velocity.\(^\text{11}\) To understand this definition it is important to know that it involves a mix of multi-structured and unstructured data. Whereas the latter is not organised or easily interpretable through traditional models (e.g. excel spreadsheets), multi-structured data is derived from interactions between humans and machines and is more difficult to interpret. Big data use massive datasets from all sorts of devices and their volume increases rapidly due to low-cost storage.\(^\text{12}\) The variety of sources from which data can be pulled contributes to this growth. Variety enables combining internal and external data to raise novel conclusions.\(^\text{13}\) Due to velocity, data which are ‘in motion’ and ‘in rest’ can be analysed which speeds up the process of data analytics. Once correlations between data have been identified with the use of an algorithm, new algorithms can be applied to derive novel information. This is called ‘machine learning’. Big data therefore enable the derivation of new information by combining different sources of different kinds of data, on a massive scale.

Big data do not have to, but often do involve personal data which are either collected or repurposed through the use of efficient algorithms. Examples of the use of personal data in

\(^{10}\) A term used for a society where the creation, distribution, use, integration and manipulation of information is a significant economic, political and cultural activity.

\(^{11}\) Definition by Gartner, IT glossary Big data. Found at: http://www.gartner.com/it-glossary/big-data/.

\(^{12}\) (Souza, et al., 2013).

\(^{13}\) (ICO, 2014), para. 25.
big data analytics are social media and loyalty cards.\textsuperscript{14} As acknowledged by the EPDS not all big data is personal but can also include aggregated data and anonymous data which do not fall within the scope of data protection law.\textsuperscript{15} The rise of big data therefore brings with it on the one hand the risk for individuals that their data are used for purposes they are not aware of and on the other hand risks for controllers and processors of those data to breach the data protection laws. The Information Commissioner’s Office (‘ICO’) also published its concerns about the possibility of big data analytics to repurpose personal data and the nature of big data to gather as much data as possible.\textsuperscript{16} According to Herold big data analytics are not a 100% accurate.\textsuperscript{17} This could result in bad decision making by companies, negatively affecting a data subject. Additionally, big data analytics could increase online discrimination. For instance, a bank could be inclined to turn down a loan when it can deduce race or behavior from a wide variety of data.

Despite these risks, big data can also bring with it clear social benefits. According to Neelie Kroes\textsuperscript{18} for citizens, data is the key to more information and empowerment and to new services and applications.\textsuperscript{19} The combination of different sets of data can improve all sorts of social or economic issues such as tailored healthcare or ensuring ‘smart’ cities that use data to reduce energy costs or crime rates.

While the benefits of big data can be multifold, it should not result in the detriment of privacy. Big data should therefore be used in a controlled manner. The use of personal data is regulated by the data protection law. To ensure we can benefit from big data while protecting privacy, it is important that data protection law is applicable in new, fast-changing environments. Concerns about data-driven technologies and business models have led the European Union to re-evaluate the current data protection framework as will be discussed below.

\subsection*{1.1 The introduction of the Data Protection Regulation}

In January 2012, the Commission proposed a reform of the EU personal data framework by introducing a proposed data protection regulation. Its objective is to give individuals back

\begin{footnotesize}
\begin{itemize}
\item\textsuperscript{14} (ICO, 2014), para. 9.
\item\textsuperscript{15} The Report, para. 7.
\item\textsuperscript{16} (ICO, 2014), para 10.
\item\textsuperscript{17} (Herold, 2014).
\item\textsuperscript{18} Vice-President of the European Commission responsible for the Digital Agenda.
\item\textsuperscript{19} Speech by Kroes, ‘The Economic and social benefits of big data’ on 23 May 2013.
\end{itemize}
\end{footnotesize}
their control over their personal data and to provide a stronger and more coherent framework to address new challenges to the protection of personal data resulting from the ‘rapid technological developments and globalization’. The Regulation introduces several drastic changes to the Directive (currently in effect) (to be discussed in Chapter 2) and will bring even greater harmonization due to its directly binding nature.

Interestingly, while the Regulation has been drafted due to rapid technological developments, it still adheres to the principles laid down in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (‘Convention’) of 1980. The protection of personal data was for the first time guaranteed in this Convention. The principles introduced by the Convention have been considered to be outdated and to provide little protection to data subjects these days. However, ICO has stressed in its report that it does not accept the argument that the data protection principles are not fit for a big data world. It stresses that ‘big data is not a game that is played by different rules’, and emphasizes the flexible nature of the principles laid down in the Directive and Regulation.

On 14 April 2016 the Regulation was given its final approval by the European Parliament, and will be applicable two years after its publication. Before going into details, I will first describe the basics of data protection law by describing i) what qualifies as personal data, ii) who controls or processes personal data and iii) under what grounds personal data can be processed.

1.2 Personal information

Personal data are defined as ‘any information relating to an identified or identifiable individual (‘data subject’). An identifiable person is someone who can be identified directly or indirectly, even by e.g by reference to an online identifier or location data. Whether an individual can be identified depends on ‘all the means likely reasonably to be used either by the controller or by any other person to identify the said person’.

---

20 Recitals 6 and 7 Regulation.
21 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28/01/1981.
22 (Moerel, 2015).
23 (ICO, 2014), para 16.
24 ibid.
26 Article 4(1) Regulation.
27 Recital 26 Regulation.
likelihood that someone can be identified is not enough. It is necessary to consider the means that may be used to identify someone. The more data available, the higher the chance that an individual can be linked to those data. Due to increasing use algorithms the likelihood of that an individual can be identified has become higher.

The Regulation is not applicable to data rendered anonymous in such a way that it cannot be used to identify an individual. However, the use of extensive algorithms on huge piles of anonymous data can enable the re-identification of an individual. Over the last couple of years it has been shown that anonymized data can easily be re-identified and linked to specific individuals. Computer scientists have even claimed that when a regulation speaks of anonymized data it is ‘violently disconnected from the best theories we have in computer science’. When combining data from databases with a variety of information, it is likely not all information has been properly made anonymous, hence, an individual could be identified.

For the sake of efficiency of the anonymised data exemption, companies ought to mitigate the risk of re-identification. In my eyes, the Regulation should have included stricter guidance to anonymising data. According to the Article 29 Working Party (‘WP29’) anonymisation should not be seen as a ‘one-off exercise’. Controllers should, in my opinion, be instructed to control the risks related re-identification regularly.

1.2.1 Sensitive personal data
A specific type of personal data is sensitive personal data. The categories of sensitive data are broad and include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex life and sexual orientation, genetic data and biometric data (known as ‘sensitive data’). Stricter conditions apply to the processing of sensitive data. Under the Regulation, a data subject will have to give explicit consent for the processing of his or her sensitive data. Explicit consent entails actively responding to an available option for data subjects to agree or disagree to certain processing. For non-sensitive data, data subjects will have to give unambiguous consent as will be discussed in paragraph 1.4.1.

28 (Ohm, 2010).
29 (Doctorow, 2013).
31 Article 9(1) Regulation.
1.3 Controller vs processor

The one who determines the purposes and means of the processing of personal data, alone or jointly with others, is considered a controller.\(^{33}\) The controller is responsible for the processing of personal data being compliant to the principles and to base the processing on a legal ground.\(^ {34}\) In order to do so, the controller is obliged to provide the appropriate technical and organizational measures and take the appropriate action in accordance with requests from data subjects. Controllers often instruct processors to process data on their behalf. The processor is limited by the instructions given to him by the controller. Such instructions are to be governed by a contract or other legal act.\(^ {35}\)

Whereas processors under the Directive are not to fear being held liable for non-compliant data processing, this has changed under the Regulation. With the introduction of joint liability for breaches of the Regulation, the relation between controller and processor and their responsibilities will have to be laid down in detail.\(^ {36}\) Data subjects also have the right to claim compensation from both controllers and processors.\(^ {37}\) Controllers will be held liable for the damage caused by non-compliant processing. Processors can only be held liable for the processing which is not in compliance with obligations under the Regulation or contrary to their instructions.

With the introduction of increased liability and high penalties for breaches,\(^ {38}\) the Regulation provides more incentive for companies to abide to data protection law. The fear for a lack of control over personal data due to big data analytics is thus partially captured by the Regulation providing better safeguards and stronger deterrents that companies do not take advantage of the loss by increased accountability.

1.4 Legal grounds for processing

Big data analyses raise questions regarding the grounds of legal processing. Without a legal ground, processing is not allowed. There are six grounds on which a data controller can rely: (i) consent, (ii) when processing is necessary for the performance of a contract, (iii) when processing is necessary for compliance with a legal obligation, (iv) when processing is  

---

\(^{33}\) Article 4(7) Regulation.  
\(^{34}\) Article 5(2) and 6 Regulation.  
\(^{35}\) Articles 26(2) and 27 Regulation.  
\(^{36}\) Article 79 Regulation.  
\(^{37}\) Article 82 Regulation.  
\(^{38}\) Article 83(4) and (5) Regulation.
necessary in order to protect the data subject’s vital interests, (v) when processing is necessary for the performance of a task carried out in the public interest and (vi) when processing is necessary for the purposes of the legitimate interests pursued by a controller.\(^{39}\)

Even though the Regulation does not specify a hierarchy in legal grounds, consent has often been considered to be the main legal ground. Mainly because it is linked to the idea that it gives data subjects control over their data and relates to the notion of information self-determination.\(^{40}\) This notion has been introduced by the German Federal Constitutional Court (‘FCC’) in 1983 in the *Census Decision*.\(^{41}\) In that decision the FCC prohibited handling of personal data unless the data subject has given consent or specific authorization is given. Self-determination guaranteed ‘the authority of the individual in principle to decide for himself whether or not his personal data should be divulged or processed’.\(^{42}\)

In light of big data, I will limit myself to focus on the grounds of consent and the legitimate interests of the controller. As I will argue in the next paragraph, consent may become obsolete in a world in which data subjects are not aware what they are consenting to. Therefore, the legitimate interests of the controller could play a more central role.

1.4.1 Consent

Consent is defined as ‘any freely given specific and informed indication’ of a data subject’s wishes to have his personal data processed.\(^{43}\) The way in which consent has to be expressed has been highly debated as the form of indication is not defined. WP29 argues that ‘any indication’ implies that an action of the data subject is required by which he signifies his wishes.\(^{44}\) Passive behavior would not be valid according to this reasoning. While many expected the Regulation to require explicit consent for processing of all kinds of personal data, the way in which consent has to given under the final text remains unambiguous although it has been clarified that consent requires ‘a clear affirmative action’.\(^{45}\) It is also necessary that the request for consent is presented to the individual in an intelligible and easily accessible form using clear and plain language.\(^{46}\)

\(^{39}\) Article 6(1) Regulation.

\(^{40}\) Introduced by the German Federal Constitutional Court as *the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others*.


\(^{42}\) The essence of this right can be found in Regulation, e.g. through the right of data portability.

\(^{43}\) Article 4(11) Regulation.

\(^{44}\) WP29 Opinion 15/2011, page 11.

\(^{45}\) Article 4(11), recitals 42-43 Regulation.

\(^{46}\) Article 7 Regulation.
When some of the data in big data analytics concerns sensitive data, data subjects will have to explicitly consent to processing of those data. This could result in a combination of legal grounds. Whereas the controller might be able to rely on his legitimate interests for ‘normal’ personal data, it will have to get explicit consent for sensitive data.

With a focus on consent, too much reliance is laid on rational behavior of data subjects. Such reliance denies the simple rule that consent triggers ‘routinisation’ of ticking boxes without proper awareness of the consequences.\(^{47}\) Often, consent is misused for the collection of personal data that would not have passed the legitimate use test, this is acknowledged by WP29.\(^{48}\) Furthermore, consent does often not even fulfill the requirement that it should be freely given when individuals are not given the choice to reject the processing. This risk has been captured by the Regulation in which is mentioned that when there is a clear imbalance between the data subject and the controller, consent should not provide a valid legal ground as it will be unlikely consent is freely given in that situation.\(^{49}\) In the Commission’s version of the Regulation this was even incorporated in the provision on consent.\(^{50}\) Whereas the Commission’s text stipulated that consent for data processed in the employment context might not be freely given, the latest draft only mentions the situation in which data is processed by a public authority. What situations result in an imbalance is not clear from the Regulation and threatens the utility of consent according to Cooper.\(^{51}\)

Of course, I think there will always be situations where freely given and specific consent will be appropriate and the only way to use people’s information. However, these situations are limited and must be, in my opinion, narrowly construed to ensure the validity of the consent.

While all the other legal grounds require the processing to be ‘necessary’, this is not mentioned in the consent ground. This does not mean that the consent releases the controller from its obligation to comply with the principles of fairness, necessity and proportionality. Data controllers will still have to balance their interests with those of the data subject. This would not make the consent ground any different than the legitimate interest ground apart

\(^{47}\) (Moerel, 2014), page 24.
\(^{49}\) Recital 43 Regulation.
\(^{50}\) Article 7.4 Regulation, version of 2012 (Council).
\(^{51}\) (Cooper, 2011).
from the consent request. Due to the interruptive and ambiguous nature of consent, I am of the opinion that the consent ground should be limited to those situations in which processing of data could negatively impact the data subject or when sensitive data is processed. Under ‘negative impact’ I define processing that ‘is likely to result in a high risk for the rights and freedoms of individuals’ such as physical, material or moral damage to individuals (among others, discrimination, identity theft or fraud, financial loss, damage to reputation). This criteria is used for the data breach notifications\(^{52}\) and will therefore, fit well under the Regulation.

In my eyes the use of consent as legal ground does not fit well with big data analytics. Big data analytics can take place online and offline, e.g. through wifi tracking while walking on the street. In such situations obtaining consent is not always possible for data controllers. I suggest that when the analysis is used to require data for objectives that have no or limited impact on the privacy of data subjects, consent would not be necessary. However, when sensitive data are used or when the analysis can negatively impact (as described above) individuals’ privacy, accordingly, explicit consent and unambiguous consent would have to be required. This would require data controllers to assess, beforehand, the possible consequences of their big data analysis on the data subjects. It necessitates a risk-based consent assessment. This risk-based approach can be found in the Regulation. Controllers are to assess the risk linked to the processing beforehand and act upon their evaluation. They are obliged to implement appropriate technical and organisational measures to mitigate the risks and to adopt the notion of protection by default and by design.\(^{53}\) These obligations provide a safety net for the situation where processing is not based on consent. Even when an individual has not consented, he or she can still expect the risks of such processing to be minimum.

1.4.2 Legitimate interests

The ground of legitimate interests of the controller could play a significant role for big data analytics. Processing is legal when it is necessary for the legitimate interests of a controller or of any third party to whom the data is disclosed, provided those interests are not overridden by the interests or fundamental rights of data subjects.\(^{54}\) This ground therefore requires a balancing test. Even though WP29 points out the benefits of the legitimate interests ground, it

---

\(^{52}\) Recital 75 and 85 Regulation.

\(^{53}\) See for example Article 32 and 35 Regulation.

\(^{54}\) Article 6(1)(f) Regulation.
also explicitly states that it should not be seen as a preferred option.\textsuperscript{55} In my opinion, however, this ground will remove many of the obstacles and complaints with regard to consent, while providing more safety to data subjects.

According to Moerel the legitimate interests ground has to be the central and only legal ground. Instead of having separate grounds based on contract or public interests, Moerel suggests that the controller will have to take account of such contextual factors when balancing interests. WP29 has given guidance on how to carry out such a balancing test in its Opinion 06/2014. A legitimate interest must (i) be lawful, (ii) be sufficiently specific and (iii) not be speculative.\textsuperscript{56}

The balancing test requires controllers to balance their or a third party’s interests with those of the data subjects. Once again, a risk-based approach as described above provides a good solution. When the processing poses privacy risks, the legitimate interests of data subjects ought to be given priority. When this is the case, their unambiguous consent is required or their explicit consent is required where sensitive data are processed.

For the processing of personal data for big data analytics I therefore propose a combination of the two abovementioned grounds. Such a combination still gives data subjects a certain level of control, through consent, over their personal data, while it is limited to those situations where processing could have a negative impact. The combination furthermore respects the many advantages of big data analytics by relying on the data controller balancing their interests and those of data subjects and giving the latter priority where the risk for privacy is high.

1.5 Data protection principles

In accordance with the Regulation, data processing has to abide by certain principles. These principles have been derived from the Convention and, while they have taken shape over the years, they have remained the same. However, times have changed significantly and it is likely that the processing of personal data by many controllers will not be in line with these principles. It has even been argued that big data is ‘antithetical’ to the principles of data processing.

\textsuperscript{56} \textit{ibid}, page 29.
minimization and purpose limitation. In this paragraph I will discuss this potential antithetical nature of big data with several of the principles.

1.5.1 Fair and legitimate processing

The first principle of the Regulation is the principle of fairness. Even though this principle can be found in multiple documents including Article 8(2) of the Charter of Fundamental Rights of the European Union, it has not received any particular information as to the scope of the required fairness. Recital 38 of the Directive tries to explain what is fair: the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection. According to this recital, fairness appears to be linked to a certain level of information that needs to be given to the data subject, that is transparency. The Regulation does not specifically mention the term ‘fairness’ but requires data to be processed ‘lawfully, fairly and in a transparent manner in relation to the data subject’.

The fact that ‘fairly’ and ‘transparent manner’ are mentioned apart from each other implies that fairness under the Regulation is broader than under the Directive. This broader vision also stems with case law of the European Court of Human Rights and the Council of Europe’s handbook. According to the Handbook fairness also requires trust, meaning that data subjects must be in a position in which they actually understand what is happening to their data. As Bygrave states, data controllers must take account of the reasonable expectations and interests of data subjects. Secret processing operations or unforeseeable negative effects are not fair. Furthermore, the legitimate interests of the data subjects must be central to the controller and the latter must ‘go beyond mandatory legal minimum requirements of service’

to inform the data subject. Bygrave also suggested that the requirement of fair also implies that companies do not pressure individuals into disclosing their data.

When Microsoft offered its latest upgrade free of charge, over 14 million users downloaded Microsoft 10 within 24 hours after its release. Understandably, the fact that such an upgrade is free of charge attracts the attention of the Microsoft users. However, consumers were actually

---

57 (Polonetsky and Tene, 2013), page 242 and 259; (Moerel, 2014), page 53.
59 Article 5(1)(a) Regulation.
60 (Council of Europe, 2014).
61 (Bygrave, 2001).
62 (Council of Europe, 2014), page 75.
63 (Bygrave, 2001).
agreeing to have Microsoft "access, disclose and preserve personal data, including your content (such as the content of your emails, other private communications or files in private folders), when we have a good faith belief that doing so is necessary to protect our customers or enforce the terms governing the use of the services." Since the collection and use of the data had to be transparent in light of the effect of the processing and the expectations of the data subjects, Microsoft did not act in line with the transparency principle nor with consumer protection law as such a clause can constitute an unfair contract term.\footnote{e.g. the French Consumer Protection Panel indicated that it is misleading for controllers to tell consumers a service free when in fact the service is provided in exchange for personal data, see (Maxwell, 2015).} Hence, fairness under consumer protection law might influence how fairness as a data protection principle should be applied.

The Regulation introduces increased transparency obligations. Controllers will have to provide transparent and easily accessible information relating to the processing when they obtain the data. This information should be in clear and plain language. The Regulation proposes the use of standardized icons to give a meaningful overview in an ‘easily visible, intelligible and clearly legible way’.\footnote{Recital 60 Regulation.} This proposal shows that big data does not have to be antithetical to the principle of fairness as long as creative and achievable steps are given to companies.

\section*{1.5.2 Principle of minimality}

Controllers are obliged to limit the collection of personal data to data that is directly relevant and necessary for the specific purpose(s). In addition, they should not retain the data longer than necessary.\footnote{Article 5(1)(c) Regulation.} The value of big data, however, is the collection of huge piles of data out of which useful information can be derived for future purposes. This is contrary to the requirement of direct relevancy.

Moerel has argued that the obsolete nature of this principle should be deleted from the Regulation.\footnote{(Moerel, 2014), page 55.} On a different note, ICO stresses the inherent flexibility of the principles which would be an argument against such deletion. The principle might be stretched as far to include data that is not strictly limited to the purposes for which it is collected for when the relevant nature of such data for compatible purposes can be shown. This links the principle of
minimality to that of purpose limitation according to which data may not be further processed in ways incompatible with the original purposes.\textsuperscript{68} Hence, entire abandonment of the minimality principle would be too radical in my eyes.

1.5.3  \textit{Purpose limitation}

According to the purpose limitation principle, personal data should be ‘collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes’.\textsuperscript{69} Purpose specification is one of the cornerstones of the EU data protection framework. Controllers are restricted in their use of the personal data they collect. The purpose must be specified before the data are collected. Purposes must be clear and specifically identified. Vague terms such as ‘marketing purpose’ or ‘research’ are often not specific enough to pass the test.\textsuperscript{70} Specification goes hand in hand with the requirement of explicitness. Clear and unambiguous specification of the purpose brings the data subject’s expectations of the use of data closer to the expectations of the controller. The last requirement is that personal data are collected for legitimate purposes only. A purpose is legitimate if it is based on one of the legal grounds laid down in Article 6 of the Regulation.

The main goal of this principle is to inhibit so called ‘function creeps’. Function creep means the situation in which a system developed for one specific purpose can be used for a variety of other purposes.\textsuperscript{71} This principle, however, is not future proof. Many companies will collect data in order to deliver the service in a later stage. Instead of collecting the data while executing the service, data forms the basis for one or many services yet to be executed. According to Moerel, \textit{‘the added value of big data resides in the potential to uncover new correlations for new potential uses once the data have been collected which may have nothing to do with the original purposes for which the data were collected’}.\textsuperscript{72} The principle of purpose limitation therefore relies on an old-fashioned concept of data processing.

To say that big data is antithetical to the principle of purpose limitation, however, ignores the inherent flexibility of this principle. Throughout the legislative process, the scope of the principle in light of further processing has been controversial. The Council had proposed to allow further processing for incompatible purposes on the ground of its legitimate interests if

\textsuperscript{68} Article 5(1)(b) Regulation.
\textsuperscript{69} Article 5(1)(b) Regulation.
\textsuperscript{70} WP29 Opinion 03/2013 on purpose limitation, 2 April 2013, page 16.
\textsuperscript{71} (Curry, et al., 2004).
\textsuperscript{72} (Moerel, 2014), page 53.
these interests outweigh those of the data subject. However, after significant concerns this provision has been left out. In the final text, further processing of data is allowed when the purposes are not incompatible with the original purpose. If that is the case, no separate legal basis is required other than the one which allowed the collection of data in the first place. Hence, further processing based on the legitimate interests is allowed, but, the purposes do have to be compatible with the original purpose. According to WP29 the regulators intended to give some flexibility with regard to further use. The Regulation includes a list of factors the controller has to take into account to ascertain whether further processing is not incompatible, such as i) the link between the purposes; the relationship between the controller and the individual and the individual’s reasonable expectations. According to ICO the key factor in deciding whether a new purpose is compatible is whether it is fair. I agree, most of the factors linked to further processing as listed in the Regulation can relate to the fairness principle. As I have discussed above, the fairness principle entails that data subjects are in a position in which they actually understand what is happening to their data so they can act upon their further use. Hence, being more transparent, also about possible further processing, is key for controllers. Therefore, I do not agree that big data analytics is antithetical to the principle of purpose limitation.

1.6 The shortcomings of data protection law
According to Koops the letter of EU data protection law is stone-dead. He considers the main aim of the Regulation to give individuals back their control over their data a delusion. He finds the focus on consent for big data analytics theoretical and meaningless. I agree with Koops that consent does not give data subjects back their control over their data, however, in combination with the legitimate interests ground and increased accountability of controller, consent can still be valuable. As I have argued in this Chapter, the focus for processing of personal data for big data analytics should rest on the combination of consent and legitimate interests. A risk based approach would reduce the need to require consent while controllers do

---

73 Article 6(4) Regulation, version of 2012 (Council).
74 (Moerel, et al., 2015).
75 Belgium, France, Poland, Malta, Italy, Hungary, Austria, Estonia, Bulgaria, Cyprus, and Lithuania all expressed reservations during the vote on the Council’s General Approach on 15 June 2015. WP29 issued a statement that it is “very much concerned” about this aspect of the Council's proposal. See the WP29's press release of March 17, 2015, on Chapter II of the GDPR at http://src.bna.com/b64.
76 Article 5(1)(b) Regulation.
77 Recital 50 Regulation.
78 WP29 Opinion 03/2013, 2 April 2013, page 11.
79 Article 6(4)(a) Regulation.
80 (ICO, 2014), page 22.
81 (Koops, 2014), page 2.
respect data subjects’ interests. This approach brings, I think, more balance between the benefits and concerns of big data analytics.

With regard to the data protection principles, some have argued that at least a few should not be applied to big data processing.\(^{82}\) Especially the principles of minimality and purpose limitation would not be ‘fit’ for big data. While it is true that big data challenges these principles, I agree with ICO that they are flexible in such a way that they could be made fit for a big data world without sacrificing big data efficiencies.

The doubts as to the relevancy of the principles requires a more modern, flexible, creative and innovative way.\(^{83}\) In addition, they must be complemented by other principles especially designed to address the issues resulting from technological developments. In the following Chapter I will discuss in what way newly introduced principles and rights in the Regulation aim to increase the control of data subjects.

**Chapter 2  Extended rights for data subjects**

No single ‘provision of control’ can be found in the Regulation.\(^{84}\) Instead, the Regulation contains several individual rights which provide individuals the possibility to exercise control over their data to a certain extent. These strengthened rights aim at giving individuals more control, including through (i) easier access to their data\(^{85}\), (ii) the right to have their data rectified or erased\(^{86}\) or to restrict their use\(^{87}\) and to (iii) have their data transferred from one controller to another.\(^{88}\) The focus on enhancing individual control has also stimulated the discussion on property over personal data.\(^{89}\) Property rights place the emphasis on the alienability and divisibility of those rights.\(^{90}\) Arguments in favor and against propertisation are diverse.\(^{91}\) For example, on the one hand property would create more effective tools of accountability and monitoring.\(^{92}\) On the other hand, it has also been argued that it

---


\(^{83}\) (EDPS, 2016), para. 6.1.

\(^{84}\) (Purtova, 2014), page 12.

\(^{85}\) Article 15 Regulation.

\(^{86}\) Article 16 and 17 Regulation

\(^{87}\) Article 18 Regulation.

\(^{88}\) Article 20 Regulation.

\(^{89}\) For instance by Purtova in (Purtova, 2015) and Orla Lynskey in (Lynskey, 2015).

\(^{90}\) (Schwart, 2004), page 2059.

\(^{91}\) See for an overview of pro’s and cons of property rights in personal data (Prins, 2006).

\(^{92}\) (Purtova, 2011), page 14.
overestimates the ability of individuals to make competition decisions.\textsuperscript{93} I will not go into
details about the desirability of propertisation. Instead, I will address the notion that several
introduced rights in the Regulation lend themselves to a property based concept.\textsuperscript{94} A quasi-
property model, as described below, ensures that data subjects can exert a level of control
while not having full control. This partial property-control could stimulate the use of personal
data in a controlled and safe way.

2.1 Data as property

Since the early 70’s\textsuperscript{95} scholars, especially from the US, have debated on the question whether
personal data should be considered property. Lessig is one of the renowned proponents of
creating a free market for personal data. Under his theory consumers can bargain with data
users before selling their data to them. This theory has been criticized because, as discussed in
the previous chapter, consumers are often blind with regard to the real value of their data,
compromising their privacy.\textsuperscript{96} To overcome such concerns Schwartz has proposed a model
that helps fashion a market that respects privacy and helps to maintain a democratic order.\textsuperscript{97}
In his eyes property should be understood as a bundle of interests instead of a dominion over
a thing.\textsuperscript{98} Ironically, Sparapani, former Public Policy Director of Facebook, endorsed
Schwartz for his theory and proposed his own quasi-property model.\textsuperscript{99}

Even though the Regulation has a human-rights-oriented approach,\textsuperscript{100} several notions laid
down in the Regulation resemble principal features described by Schwartz’s criteria.

2.1.1 Default rules

According to Schwartz alienability of personal data means the ‘restriction on the use of
personal data combined with a limitation on their transferability’.\textsuperscript{101} Under the Regulation,
data subjects have the right to erasure, removal and the right of data portability. These
requirements ensure the notion that data subjects maintain default entitlements to their data.
For example, a data subject may exercise his or her right to erasure without undue delay

\textsuperscript{93} (Lynskey, 2015), page 252.
\textsuperscript{94} (Victor, 2013).
\textsuperscript{95} See e.g. (Westin, 1968).
\textsuperscript{96} (Lessig, 2002), page 256.
\textsuperscript{97} (Schwartz, 2004), page 2056.
\textsuperscript{98} (Schwartz, 2004) page 2094.
\textsuperscript{99} (Sparapani, 2012).
\textsuperscript{100} Q. and A. with Viviane Reding, N.Y. Times, February 2, 2013, found at:
\textsuperscript{101} (Schwartz, 2004), page 2095.
requiring the controller to erase the data when, among others, (a) the data subject withdraws his or her consent and no other legal ground exists or (b) the data subject objects to the processing in accordance with his or her right to object\textsuperscript{102} and no overriding legitimate grounds exists.\textsuperscript{103} The right to object can be exercised at any time when, among other, the processing is based upon the ground of legitimate interests of the controller or where the data are processed for direct marketing purposes.\textsuperscript{104}

Furthermore, data subjects have the right to obtain from the controller restriction of processing, though limited to certain conditions.\textsuperscript{105} A restriction imposed on the controller obliges him to only process the data with the data subject’s consent, the establishment, exercise or defence of legal claims, for the protection of other person’s rights or for reasons of public interests of the EU or Member State.\textsuperscript{106}

With this in mind, it can be argued that the Regulation is based on the assumption that data is capable of changing hands although the ultimate control is exercised by the data subject.\textsuperscript{107} Schwartz proposes a hybrid form of alienability restriction on personal data. This hybrid form permits the transfer for an initial category of use but only when the data subject has the opportunity to block further transfer or use. Other use would require the data subject to ‘opt-in’, or in terms of the Regulation the data subject’s consent.\textsuperscript{108} The combination of rights in the Regulation resemble this hybrid form.

2.1.2 Inalienability of personal data

Property rights ‘run with’ the object.\textsuperscript{109} According to Schwartz, use-transfer restrictions have to run with the data to limit the market failures associated with the situation in which individuals ‘trade away too much of their propertised personal information’.

Under the Regulation, data subjects have the explicit right to demand erasure of the data from the controller that subsequently has to take all reasonable steps to inform other controllers
who are processing the data to erase any links to, copy or replication of those data as well.\(^{110}\)

When a data subject restricts the processing or uses his or her right to erasure or rectification, the relevant controller shall communicate this to each recipient to whom the data have been disclosed. Only when this proves impossible or involves disproportionate efforts, will such obligation not be applicable.\(^{111}\)

The Regulation thus provides for the ability of use-transfer restrictions to run with the data. Any controller or recipient must respect these restrictions, even though they have no direct relation with the data subject.

### 2.1.3 Remedies

With respect to privacy violations, Schwartz prefers damages to be set by the state. To rely on the data sellers and buyers to set the price for violations would, in his eyes, produce inadequate deterrence.\(^{112}\) The damages should furthermore be set high because (i) actual damages are often hard to show (ii) personal data of one person may not have enough value to justify litigation and (iii) it is difficult to detect violations.\(^{113}\)

The remedies available under the Regulation seem to adhere to this idea. Data controllers and processors can face administrative fines of up to EUR 20.000.000,\(^{-}\), or up 4% of their annual worldwide turnover\(^{114}\) when they do not comply with e.g. the right of erasure or the lack of a sufficient legal ground.\(^{115}\)

### 2.2 Self-determination

The abovementioned rights introduced by the Regulation provide, I think, better control for data subjects over their data. Where I have advocated for less use of consent as a legal ground in Chapter 1, the rights of erasure, rectification and restrictions diminish the possible decrease of self-determination that is inherent to consent. In the end, it are the data subjects that determine what happens to their data while they are not granted all the sticks as would have been in the case in a true property-based system. This way, third party interests are taken into account and the use of big data analytics is not significantly restricted.

---

110 Article 17(2) Regulation.
111 Article 19 Regulation.
112 (Schwartz, 2004), page 2108.
113 ibid, page 2109.
114 In case the controller is an enterprise.
115 Article 83(4) and (5) Regulation
2.3 Profiling

While I am satisfied with the introduction of the abovementioned rights, there is one important provision in the Regulation I am not too content with. This involves profiling. In addition to the abovementioned rights, the Regulation provides for an explicit provision on profiling due to increasing technologies enhancing the ability to profile. Profiling is defined as ‘any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements’.

Profiling enables controllers to build profiles of individuals over time. Such profiles can later be used for different purposes such as marketing or credit-referencing. This has significant impact on the control data subjects can exercise over their data, especially since most profiling happens without their knowledge. To mitigate these risks, the data subject will have to give his or her explicit consent.

Article 22 Regulation gives data subjects the right not to be subject to decisions based solely on automated processing which produce legal effects concerning him or her or significantly affects him or her. Due to the broad scope of profiling a lot of processing activities would fall under the category profiling. Only profiling that produces legal effects concerning or significantly affects data subjects requires the explicit consent of a data subject. This ‘significant affect’ appears to be a rather high threshold and no clarification on its scope can be found in the Regulation.

On first sight, the prohibition provides individuals sufficient control over the use of their data for profiling. However, without a clear indication what can be qualified as ‘significantly affect’ an individual’s right, the provision could be a toothless dragon. This provision might be a hurdle on the way to provide data subjects more and better control. Let’s hope either the ECJ or the European institution themselves take it upon them to clarify this provision.

---

116 Article 4(3)(aa) Regulation.
118 Article 22(2)(c).
119 Article 20(1) Regulation, or any of the other grounds mentioned in this article.
Chapter 3  Abusive nature of control over personal data

3.1  Privacy or competition

You might have wondered where in the discussion on control over personal data, competition law comes into play. You have come to the part where I will step from EU data protection law to EU competition law. In the following chapters I will address how competition law could play a part in ensuring that the control over data remains with the individuals.

Privacy advocates have argued that competition law ought to take into account privacy as ‘privacy harms can lead to a reduction in the quality of a good or service, which is a standard category of harm that results from market power. Where these sorts of harm exist, it is a normal part of antitrust analysis to assess such harms and seek to minimize them’. Sophie in ‘t Veld, stated that the reason for companies to have data is because it gives them a competitive advantage. Therefore, the two fields of law cannot be disconnected. According to the EDPS, this competitive advantage could result in market foreclosure, due to the incapability of small market players to acquire the same bulk of data. Proponents of the assessment of privacy under competition law argue that such would result in an undesirable level of uncertainty as to the economic scope of competition law.

I agree with Margareth Vestager that we do not need a ‘new competition rulebook for the big data world’. However, she also mentioned that, while no competition problems have occurred yet, it does not mean they never will. In this light, the investigation by the Bundeskartellambt could set an important precedent. In the following paragraphs I will discuss how competition law notions might be used for privacy concerns related to personal data and whether this should be possible in the future.

---

120 Behavioral Advertising: Tracking, Targeting, and Technology: Town Hall Before the FTC, (Oct. 18, 2007) (testimony of Peter Swire, Professor, Moritz College of Law of the Ohio State University).
121 EDRI, European Parliament hearing on Internet privacy issues, 30 January 2008, found at: https://edri.org/edrigramnumber6-2ep-hearing-privacy/.
122 The Report, page 3.
124 Speech by M. Vestager on 16 January 2016, see footnote 4.
3.2 Competition based on quality

EU competition law deals with the behavior of companies and abuse of market power. Its principal aims are to enhance the functioning of the internal market and the welfare of and available choices to consumers.\(^\text{125}\) The general rules of EU competition law are laid down in Articles 101 and 102 of the Treaty of the Functioning of the European Union (‘TFEU’).\(^\text{126}\) Under Article 101 TFEU any agreement or concerted practice made between two or more undertakings, which affects trade between Member States and which has the object or effect of restricting competition is prohibited. Article 102 TFEU prohibits the abuse of market power by an incumbent. In addition to the TFEU, EU competition law includes the EU Merger Regulation which prohibits mergers and acquisitions between undertakings which would significantly reduce competition on the relevant market.

Even though Articles 101 and 102 TFEU do not specify any hierarchy of competitive parameters, the focus has mainly been on price.\(^\text{127}\) However it is acknowledged that quality is often more important than price.\(^\text{128}\) In its *Intel* decision the Commission noted that there may be no single factor defining quality.\(^\text{129}\) Due to difficulties in evaluating quality factors based on quantitative assessments, quality is often assessed by qualitative tools such as questionnaires or interviews.\(^\text{130}\) The role of quality effects has even been described as one of the most vexatious and still unresolved issues.\(^\text{131}\) However, it has been proposed that the conditions under data protection law can provide a yardstick for assessing quality under competition law.\(^\text{132}\)

Data have a certain economic value. Data are, however, different from many other input factors. Data are by nature non-rivalrous, meaning a data subject can give their data over and over again without extorting them. Data given to one company do not distract a competitor from the same data. To describe personal data as the new oil or the new currency is therefore misleading. The fact that personal data have a value and the efficiencies companies can reap

---


\(^\text{127}\) (Ezrachie, et al., 2015).

\(^\text{128}\) (OECD Competition Committee, 2013).


\(^\text{130}\) (OECD Competition Committee, 2013), page 87.

\(^\text{131}\) *ibid*, page 1.

\(^\text{132}\) (Costa-Cabral et al., 2015), page 16.
from those data, does not make it a currency. The precise value of data depends on the context and accuracy of the data.

The EDPS argues that while data are essentially non-rivalrous, companies could in practice be excluded from their utilization. Incumbents could have a certain power over their collected data which could keep possible competitors off the market (‘entry-barriers’). This is where competition law comes to play. The following paragraphs I will discuss in what ways competition law could provide data subjects another dimension of control over their data. Instead of focusing on the data subject and his or her consent, competition law focuses on keeping a level playing field for competitors on markets where products and services are provided for free in exchange of personal data.

3.3 Consumer welfare

According to case law of the ECJ, consumer protection lies at the heart of EU competition law. Where informed, educated and active consumers drive a competitive market, it is they who require protection from anti-competitive activities. Consumer welfare has for a long time been considered the ultimate goal of competition law. Remarkably though, it was only recently that the ECJ mentioned consumer welfare. In Post Danmark the ECJ repeated the formulation often used by the Commission and stated that ‘not every exclusionary effect is necessarily detrimental to competition. Competition on the merits may, by definition, lead to the departure from the market or the marginalisation of competitors that are less efficient and so less attractive to consumers from the point of view of, among other things, price, choice, quality or innovation’. The OECD standard economic definition of consumer welfare reads as follows: ‘Consumer welfare refers to the individual benefits derived from the consumption of goods and services. In theory, individual welfare is defined by an individual's own assessment of his/her satisfaction, given prices and income. Exact measurement of consumer welfare therefore requires information about individual preferences’. It is clear that it is hard to measure consumer welfare based on individual preferences. In practice it is measured by consumer surplus, a term defined by the OECD as ‘a measure of consumer welfare and is defined as the excess of social valuation of product over the price actually paid. It is measured by the area of a triangle below a demand curve and above the observed price’. Accordingly, consumer harm under this standard means a reduction in wealth due to an increase in price. Hence, welfare is expressed in price advantage. Economists have cautioned a static use of consumer surplus. Especially in light of dynamic markets in which companies strongly rely on personal data, a consumer surplus

---

134 See e.g. ECJ Case C-120/78, REWE-Zentral-AG v Bundesmonopolverwaltung für Branntwein, ECR 649, 20 February 1979.
135 See e.g. ECJ C-209/10, Post Danmark A/S v Konkurrencerådet, 27 March 2012.
136 ibid, para. 22.
137 OECD, Glossary of Statistical Terms, found at: https://stats.oecd.org/glossary/.
138 ibid.
139 (Daskalova, 2015), page 135.
140 (Kingston, 2011), page 174.
standard should not block economic growth and innovation. Both the Commission and the ECJ no longer consider consumer welfare as the primary goal of competition law. It is aligned next to other goals such as innovation and competitiveness.\textsuperscript{141} The shift in focus on consumer welfare to other goals makes it hard to think that the consumer surplus is defined narrowly. This is exemplified by the Commission’s \textit{Microsoft} decision where it’s main concern lied with the limitation of choice for consumers and innovation instead of monetary harm due to price increases.\textsuperscript{142}

### 3.4 Value of personal data

One of the key problems linked to personal data is not knowing how to value the data. Several methodologies for estimating the value have been discussed by the OECD and even though they are rudimentary, they serve as a starting point for further research. The methodologies are divided into value based on market valuation or on individuals’ valuation. One of the methodologies based on the market valuation is to evaluate the market price for data offered on the market by data brokers. This, however, does not represent the actual value since the acquirer can profit from the data for other purposes. A method based on individuals’ evaluation is to evaluate the price firms are willing to pay consumers to give up their data. The problem with this method is the incapability of individuals to value their own data, defined by Froomkin as ‘privacy myopia’.\textsuperscript{143} People differ when it comes to their individual valuation of personal data and their privacy.\textsuperscript{144} Furthermore, as will be elaborated in the next paragraph, both evaluations are sensitive to contextual effects. This issue in combination with the unclear full economic benefit derived from the data, makes it hard to truly evaluate the value of personal data.

### 3.4 Control over data

Control over one’s personal data is an important notion encouraged by the Commission. However, human beings are not good at making rational decisions when the information provided to them is complicated and they receive short term benefits whereas the costs are long term based.\textsuperscript{145}

\textsuperscript{141} Joaquín Almunia, \textit{“Competition policy for the post-crisis world: A perspective”} (Speech/14/34, 17 January 2014, Bruges, Belgium).


\textsuperscript{143} (Froomkin, 2000), 1501ff.

\textsuperscript{144} (OECD Competition Committee, 2013), page 5.

\textsuperscript{145} (Moerel, 2014), page 48.
3.6 The rise of the ‘free’

Due to a rapid growth on the marketplace of free products and services (‘free goods’), new production methods and the dissemination of personal information have become an important asset to the economy. The more common personal information is regarded as such, the more common exchanges in which personal data are regarded as a currency will be. In turn, the more free goods are available on the market, the more consumers expect to receive them in other markets. The irrational, lenient behaviour of consumers regarding their privacy have encouraged companies to profit from consumers lack of care by providing e.g. targeted ads.

The motivations behind providing free goods are diverse. It could either be a means to grow consumer demand of the good or to intrigue consumers into buying the ‘premium’ versions of the good. Research shows that a free good is so attractive than another good, even if the latter’s price has been reduced by five times or has greater value, that consumers barely picture it as two options. This ‘free effect’ creates inconsistencies between demand and quality of the goods.

Before delving into a more competition law analysis of free goods I will start from the point that ‘free’ is usually pro-competitive, hence beneficial for overall welfare. Free goods can encourage undertakings to compete on both quality and price. Furthermore, it can help newcomers to the market to overcome barriers to entry, especially when it is a market on which consumers are not likely to switch between goods. Enhance by the ‘free effect’ the provision of free goods enables companies to assess the flaws and strengths of the product and react on this, providing more enhanced goods within a short timeframe.

3.7 Abuse of market power

Article 102 TFEU prohibits abusive behaviour by undertakings that have a dominant position on a particular market (an ‘incumbent’). A dominant position ‘relates to a position of economic strength enjoyed by an undertaking, which enables it to prevent effective

146 (Shelanski, 2013); (Evans, 2013).
147 (Gal, et al., 2015), page 16.
148 (Smith, 2014); (Evans, 2009).
149 (Jacob, 2004).
150 (Nelson, 1970); (VillasBoas, 2006).
151 (Dengler, 2013).
competition being maintained on the relevant market by affording it the power to behave to an appreciable extent independently of its competitors, its customers and ultimately of the consumers.\textsuperscript{152} In other words, the undertaking must have substantial market power. If an undertaking has market power it can influence market prices, output, innovation, the variety or the quality of goods for a period of time.\textsuperscript{153} To have market power is in itself not prohibited. To abuse that position however is.

Abuse of a dominant position in relation to personal data could theoretically take form in (i) a unilateral decision to lower privacy standards, (ii) price discrimination or (iii) the failure to grant access to data where such data is considered indispensable for competitors to effectively compete. These conducts have not (yet) been considered to constitute abuse under competition law. However, with the pending research of the German Bundeskartellamt on the use by Facebook of specific terms on the use of personal data, it cannot be excluded.

\textbf{3.7.1 Lower privacy standards}

An incumbent could abuse this position by lowering its quality of data use policy. A decrease in price could be just as harmful to consumers as an increase in price. Under Article 102 TFEU ‘excessive pricing’ – directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions – is prohibited. Case law on excessive pricing is limited due to the high threshold for finding excessive pricing.\textsuperscript{154}

An incumbent could abuse its dominant position by charging excessive prices. Due to a lack of competition, it can so do. Hence, an incumbent could also excessively reduce its quality of its privacy policy when it is not constraint by competition. Such ‘excessive decrease in quality’ might be considered an abuse of market power since, just like excessive prices, it harms consumer welfare and could be defined as exploitative.\textsuperscript{155} Excessive pricing can be justified where the price is a reward for the investments the incumbent made for the free goods. Such a justification would not apply for lower quality of privacy policies. In theory exploitative decrease in quality could constitute abuse of a dominant position under Article

\textsuperscript{152} ECJ Case 27/76, United Brands Company and United Brands Continentaal BV v Commission, ECR 1978, para. 65; ECJ Case 85/76 Hoffmann-La Roche & Co. AG v Commission ECR 1979, para. 38.

\textsuperscript{153} Working Party No. 3 on Co-operation and Enforcement, Roundtable discussion on techniques and evidentiary issues in proving dominance, 7 June 2006, page 2.

\textsuperscript{154} (Fletcher, 2007).

\textsuperscript{155} Case C-247/86, Alsatel v Novasam ECR 1988.
102 TFEU. However, this would require a complex analysis when determining what decrease qualifies as excessive.

A much criticised approach would be to state that a decrease in quality of privacy policy under the required level of privacy protection under the Regulation - which is already hard to define – could constitute an excessive decrease, hence an infringement of competition law.\textsuperscript{156} The ECJ has recognized that an infringement of one area of law could be a factor in deciding that there has been an infringement of competition law as well.\textsuperscript{157} It is a factor that can be taken into consideration, not the basis on which a competition law infringement should be based. By using the data protection law regime as yardstick to assess the exploitative nature of the decrease, the scope of competition law is distorted. In Astrazeneca the ECJ noted that ‘the classification as an abuse of a dominant position of conduct [...] which consists in the use of regulatory procedures without any basis in competition on the merits, requires at the very least evidence that, in view of the economic or regulatory context surrounding that conduct, that conduct is such as to restrict competition’.\textsuperscript{158}

This approach brings with it significant consequences. Any infringement to a rule that aims to protect consumer welfare, could subsequently be considered as an exploitative abuse under competition law when the quality of the free goods is negatively affected. In light of the Facebook investigation, there may be information asymmetries regarding the use of data but this should be dealt with via data protection law as it does not affect competition or renders consumer’s choice. This difference should be clearly kept in mind when competition authorities start to mingle in privacy concerns.

The ‘excessive’ nature of a quality decrease must thus be assessed differently. I have my doubts about the level of knowledge Competition Authorities have to determine when privacy conditions are ‘excessive’. I hope the Bundeskartellamt, as the first authority to conduct an investigation, is prepared to ‘take a shortcut’\textsuperscript{159} and equate the infringement of data protection law as an infringement of Article 102 TFEU.

\textsuperscript{156} For critique see e.g. (Costa-Cabral et al., 2015), page 20; Alfonso Lamadrid de Pablo ‘Facebook, Privacy and Article 102- a first comment on the Bundeskartellamt’s investigation’, Chilling Competition, March 2016.

\textsuperscript{157} ECJ Case C-32/11, Allianz Hungaria v Gazdasági Versenyhivatal, 14 March 2014,

\textsuperscript{158} Case T-321/05, Astrazeneca v Commission, 1 July 2010, para 845.

\textsuperscript{159} As mentioned by Alfonso Lamadrid de Pablo, see footnote 147.
3.7.2 Price discrimination or other types of targeting

As mentioned in the previous chapter, data subjects will have the right not to be subject to decisions based solely on automated processing which produce legal effects concerning him or her or significantly affects him or her. In terms of competition law, behavioural profiling allows undertakings to offer goods at different prices to extract the highest price from an individual. Data collection by incumbents can facilitate price discrimination harming consumer welfare. On the other hand, the analysis of the data also provides benefits to consumers they would not have had in the absence of big data collection. Price discrimination may be pro-competitive as it provides entry incentives to competitors and it could enlarge the group of consumers reached. Customers who would not have paid a certain good or service for a price set at EUR 35 might be willing to pay EUR 30. Profiling those consumers benefit both them as the undertakings. The effects of discrimination on welfare are thus ambiguous.\textsuperscript{160}

Under Article 102 TFEU price discrimination covers a wide range of practices such as tying, selective price cuts and discounts. According to Posner the term is used to define ‘the practice of selling the same product to different customers at different prices even though the cost of sale is the same to each of them.’\textsuperscript{161} Price discrimination is complex, there is no coherent analytic framework to assess discrimination nor is there consensus about which standard of welfare is pursued.\textsuperscript{162}

Several conditions have to be met for discrimination to be abusive. First of all the incumbent must apply ‘dissimilar conditions to equivalent transactions with other trading partners’. Secondly, the discriminatory practice must put those parties at a ‘competitive disadvantage’. Thirdly, discrimination can only be considered an abuse of market power if the incumbent has the ability to prevent arbitrage or resale of the goods or service.\textsuperscript{163}

The requirements of ‘trading partners’ and ‘competitive disadvantage’ result in Article 102(c) TFEU being applicable only to discrimination between competitors. Therefore, the final

\textsuperscript{160} (Schmalensee, 2005), page 168.
\textsuperscript{161} (Posner, 2001), at 79-80.
\textsuperscript{162} (Gerardin, et al., 2005), page 6.
\textsuperscript{163} \textit{ibid}, page 5.
consumer, often the data subject, does not suffer a competitive disadvantage as he or she does not participate in competition.

Personalised pricing could therefore only be able to fall under Article 102(a) – unfair purchase pricing – which brings us back to the ambiguity of unfairness. Fairness does not provide a clear answer to the question whether profiling should be captured under Article 102 TFEU. Under the fairness principle it could be stated that it is fair when consumers with a higher income are charged higher prices. An economic perspective towards ‘fair prices’ even requires discrimination. After all, a fair price depends on the consumer’s valuation of the product. Similar to the assessment of ‘excessive’ privacy conditions, it will be a complex task for competition authorities to determine an appropriate bench rule.

3.7.3 Data portability – the heart of competition law

Personal data as ‘asset’ has led some authors to say that a refusal to supply this ‘asset’ can also constitute an abuse of dominance under Article 102 TFEU. As Almunia has stated, data portability goes ‘to the heart of competition policy’.\(^{164}\) The portability of data is important in markets where effective competition requires the ability for individuals to switch to competitors by taking their data with them. Without this possibility, consumers are less willing to switch to competitors of the undertaking used by those consumers. Hence, the right to data portability under the Regulation can positively affect competition on a market.

The notion of essential facility has been elaborated in case law of the ECJ. The conditions that apply to access to essential facilities are strict and are not so easy applicable in case of personal data as will be discussed below. The doctrine of essential facility was introduced by the ECJ in *Magill* where it found that in ‘exceptional circumstances’ third parties ought to get access to goods or services despite the existence of intellectual property rights on those goods or services.\(^{165}\) In *Bronner*, the second EU case on the doctrine, the ECJ stated that a facility should be granted to third parties when a) the refusal to deal is likely to eliminate all competition from the relevant market and b) the facility is indispensable to carrying on that parties’ business, inasmuch no actual or potential substitute exists.\(^{166}\) A facility is

---

\(^{164}\) J. Almunia, ‘*Competition and personal data protection*’, November 26, 2012, SPEECH/12/860.


indispensable when i) there is no plausible alternative, even of inferior quality and ii) the impossibility to duplicate the facility is due to technical, legal or economic (objective) obstacles.\textsuperscript{167}

According to the EDPS in its Report information can in theory be considered an essential facility because ‘the dominant undertaking has exclusive control of the information, while competitors lack the technical means to recreate the structure or system upon which the service relies. This effectively prevents entry to the market and restricts consumer choice.’\textsuperscript{168}

In another landmark case, \textit{IMS Health}\textsuperscript{169}, the ECJ found other circumstances to be of importance: i) the third party needs the facility for the introduction of a new product or service and ii) the refusal results in the incumbent reserving, the actual, a potential or a hypothetical market by eliminating all competition on that market.

All of the circumstances appear to be inapplicable in case of personal data as the essential facility. The Commission in the \textit{Google/DoubleClick} case determined that ‘data on searches with data on user’s web surfing behavior is already available to a number of Google’s competitors today’. In addition the Commission stated that data can also be purchased from third parties, which may be broader and richer than the data collected by DoubleClick.\textsuperscript{170}

Hence, it will be hard to argue that personal data is truly an essential facility. The undertaking seeking access will have to give evidence of the fact that the data is essential and cannot be developed otherwise.

Since the ‘essential facility’ doctrine under competition law cannot provide an adequate framework for the transferability of data, the Regulation should ensure the right of portability does not lose its efficiency due to possible restrictions. The Regulation introduces the right for data subjects to have his or her data transferred from the controller directly to another controller when technically feasible. To make this right as efficient as possible, and to make it less likely competition law has to step in, its scope should, I think, not be limited to situations where the transfer is ‘technically feasible’. Controllers are encouraged to develop interoperable data formats, however, this is not a binding obligation. It is odd that the

\begin{flushleft}
\textsuperscript{167} ibid, para. 44. \\
\textsuperscript{168} The Report, para. 56. \\
\textsuperscript{169} ECJ Case C-418/1, IMS Health GmbH & CO OHG v NDC Health GmbH & Co. KG, ECR 2004, 29 April 2004, para. 38. \\
\textsuperscript{170} Case No COMP/M.4731, Google/DoubleClick, 11 March 2008, para. 271.
\end{flushleft}
Commission has stated that ‘the possibility to move data from one service provider to another would increase competition in some sectors, e.g. between social networks, and could also make data protection an element in this competition’, but did not make it compulsory for controllers to ensure they are capable of transferring data to whatever format the data subject wants their data to be transferred to.

Besides, obliging a controller to transfer data under Article 102 TFEU could infringe data protection law when the ground for such a transfer is absent. It would be hard to require the consent from each and every data subject for the transfer. Also, the legitimate interests of the data subjects will most likely outweigh the interests of the company asking for the transfer (a third party).

3.8 New definition of consumer harm
To overcome the problems competition authorities will face when privacy is to be assessed under competition law, the EDPS has proposed to develop a concept of consumer harm in cases where the control and choice of personal data is restricted by an incumbent.\textsuperscript{171} Such a concept would account for risks to privacy and would not merely focus on competitive effects.

As I have mentioned before, consumer harm under EU competition law focuses mainly on a decrease in wealth due to an increase in prices. Social welfare and consumer welfare, however, entail much more than just wealth expressed in prices. Wealth also covers increases or decreases in quality or innovation as recognized by the ECJ in \textit{Post Danmark}.\textsuperscript{172} These concepts are much harder to measure. The meaning of social welfare is thus not self-explanatory and has even resulted in contradictory reasoning by the Commission and courts.

Consumer harm arises only when competitors of an incumbent are ‘prevented from bringing innovative goods or services to market and/or where follow-on innovation is likely to be stifled’ due to a refusal to supply.\textsuperscript{173} Due to the non-rivalrous nature of personal data, the real problem seems to lie in the fact that smaller market players are kept from the right algorithms or techniques, not so much from the data itself. To include privacy harm in the definition of

\begin{footnotesize}
\begin{itemize}
  \item \textsuperscript{171} (EDPS, 2014), para 4.
  \item \textsuperscript{172} ECJ in \textit{Post Danmark}, para. 22.
  \item \textsuperscript{173} Enforcement Priorities in Applying Article 102 TFEU to Abusive Exclusionary Conduct by Dominant Undertakings, OJ C 45, 24.2.2009, para. 71.
\end{itemize}
\end{footnotesize}
consumer harm would be detrimental to economic scope of competition law. In my eyes, broadening the scope is therefore undesirable. First of all, it could result in a full-fledged regulation. Competition authorities could be allowed to enforce all aspects of a market, competitive or not. The economic focus of competition law would become contested and its scope questionable. Not to mention that the rights as discussed in Chapter 2 ensure data subjects can exercise control over their personal data. Incumbents cannot escape their obligations under the Regulation. In addition, the right to data portability under the Regulation ensures that data subjects are not locked in with incumbents because the latter have their data. With the ability to take their data with them, data subjects have the choice to swift between competitors. Ultimately, as emphasized by the EDPS itself, it are the data subjects that ought to control to whom their data is transferred to.

**Conclusion**

The recognition of the instrumental and conceptual role of individual control over personal data is of the essence in a world of big data. With the approval of the Regulation, the EU has taken a significant step in enhancing the level of control data subjects can exercise over their own data. While giving back control is central to the Regulation, the importance and significance of big data analytics is also acknowledged.

Several authors have criticised the Regulation for being ‘unfit’ for a world of big data. The principles of minimality and purpose limitation would even be ‘antithetical’ to big data. The focus of these principles on limiting the collection and processing of data for specific and clear purposes would be contrary to the use and value of big data analytics. While I agree with the critics that the principles are, on first sight, outdated, they do not acknowledge the flexible nature of the principles.

Nonetheless, the possible ‘unfit’ nature of the principles is mitigated by the adoption of several quasi-property rights based rights. The right to access, erasure, rectification and data portability provide data subjects a level of control over their data almost similar to property rights. While controllers and processors may use the data, in the end it are the data subjects that control that use. In my eyes, the Regulation provides a proper balance between the interests of individuals and the interests of companies in using as much data as possible. However, the Regulation could have included more clarity on and safeguards against
anonymisation and profiling. Whether there is such a thing as truly anonymous data is questionable in my eyes. I am of the opinion that without an explicit obligation for controllers to ensure their data is and remains anonymous, the exemption for anonymous data does not provide a sufficient level of protection for individuals. As for the profiling provision in the Regulation, the lack of clarity as to what can be understood to ‘significantly affect’ an individual seems to open the door for profiling not based on the explicit consent of individuals. However, these two points do not have to have a significant negative impact due to the risk-based approach of the Regulation. The increased accountability and responsibilities for controller to ensure privacy risks create a level of protection for individuals in those cases where they might be restricted in their control. The Regulation therefore provide a sufficient level of control for individuals in a world where their data can be worth fighting for.

This competitive nature of personal data has brought about discussions concerning the need for privacy assessments under competition law. The way I see it is that privacy constitutes a relevant non-price parameter of competition. I do not disregard the situation that companies do compete on how they protect their personal data. This competitive nature of personal data would, however, be better controlled under data protection law itself. Whereas according to some the regulation is unfit for privacy concerns due to big data, I state that it is competition law that is unfit for big data privacy concerns.

First of all, unlike prices, the value of personal data is extremely hard to measure. Where data subjects are often not able to properly value their data, it seems unlikely competition authorities can. Secondly, I wonder how the competition on a certain market would be significantly affected by e.g. inefficient privacy terms. Thirdly, due to the non-rivalrous nature of personal data, the real problem would sooner lie in the fact that smaller market players are kept from the right algorithms or techniques, not so much from the data itself. Furthermore, the economic focus of competition law would become contested and its scope questionable. Last but not least, data protection appears to have included a competition friendly approach by including the right to data portability. This right can ensure a level playing field on a specific market while also respecting that the data subject itself decides where they transfer their data.

I will be anxiously awaiting the publication of the investigation on Facebook by the Bundeskartellambt. It will be interesting to see how the authority will link an infringement of
data protection law to an abuse of a dominant position. While we can see the positive influence of competition law in the Regulation\textsuperscript{174}, so might the Regulation positively influence competition law. The challenge is not to lose the main focus of both fields of law out of sight.

\textsuperscript{174} In the right to data portability.
Table of reference

Case Law
- ECJ Case 27/76, United Brands Company and United Brands Continentaal BV v Commission, ECR-00207, 14 February 1978;
- ECJ Case 85/76 Hoffmann-La Roche & Co. AG v Commission ECR-00461.
- ECJ Case C-120/78, REWE-Zentral-AG v Bundesmonopolverwaltung für Branntwein, ECR 00649, 20 February 1979.
- ECJ Case C-7/97, Oscar Bronner GmbH & Co. KG v Mediaprint, ECR-07791, 26 November 1998.
- ECJ Case C-418/1, IMS Health GmbH & CO OHG v NDC Health GmbH & Co. KG, ECR 05039, 29 April 2004.
- Case COMP/M.4731, Google/DoubleClick, 11 March 2008.
- Case T-321/05, AstraZeneca v Commission, ECR II-02805, 1 July 2010.
- ECJ Case C-32/11, Allianz Hungaria v Gazdasági Versenyhivatal, 14 March 2014.

Books and Articles
• Degli-Esposti, Sara, ‘Big Data Protection Study Report’, The Open University, April 2015.
• Evans, David, ‘Attention Rivalry Among Online Platforms’ Global Economics Group; University of Chicago Law School; University College London, 12 April 2013.
• European Digital Rights, ‘Position on the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), found at: https://edri.org/files/1012EDRi_full_position.pdf.
• European Data Protection Supervisor, ‘Executive Summary of the Opinion of the European Data Protection Supervisor on 'Meeting the challenges of big data: a call for transparency, user control, data protection by design and accountability'", Official Journal of the European Union, 20 February 2016.
• Information Commissioner's Office, ‘Big data and data protection’,version 1.0, 20140728.


• Lamadrid de Pablo, Alfonso, ‘Facebook, Privacy and Article 102- a first comment on the Bundeskartellamt’s investigation’, Chilling Competition, March 2016, found at: https://chillingcompetition.com/2016/03/02/facebook-privacy-and-article-102-a-first-comment-on-the-bundeskartellamts-investigation/.


• Moerel, Lokke, ‘How to Make the Draft EU Regulation on Data Protection Future Proof’ University of Tilburg, 14 February 2014.

• Moerel, Lokke ‘On the Death of Purpose Limitation’ Privacy Perspectives, 2 June 2015.

• Moerel, Lokke and Prins, Corien, ‘Further processing of data based on the legitimate interests ground: the end of purpose limitation?’, Tilburg University, June 2015.


• OECD Competition Committee, ‘Exploring the economics of personal data: a survey of methodologies for measuring monetary value’ Volume 5, 2 April 2013.


• Souza, Robert and Trollinger, Rob and Kaestner, Cornelius and Potere, David and Jamrich, Jan, ‘How to get started with big data. BCG perspectives’, The Boston Consulting Group, 29 May 2013, found at: https://www.bcgperspectives.com/content/articles/it_strategy_retail_how_to_get_started_with_big_data/.
• Sparapani, Timothy, ‘Putting Consumers at the Heart of the Social Media Revolution: Toward a Personal Property Interest to Protect Privacy’, HeinOnline, 2012.
• Watson, Hayley, ‘International study finds that four in ten organisations obstruct our access to our own data’, IRISS Press Release, 23 June 2014.

Regulatory documents, Reports and Opinions
• Interinstitutional File 2012/0011 (COD), Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data
and on the free movement of such data (General Data Protection Regulation), Brussels, 6 April 2016.


- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28/01/1981.


- Enforcement Priorities in Applying Article 102 TFEU to Abusive Exclusionary Conduct by Dominant Undertakings, OJ C 45, 24 February 2009.


- Article 29 Working Party Opinion 05/2014 on Anonymiation Techniques, 0829/14/EN/WP1, 10 April 2014


- Article 29 Working Party Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, 2 April 2013


