# Informational Self-Determination in Context: Privacy and Data Protection in the Age of Big Data and Surveillance Capitalism

Thesis submitted in fulfilment of the requirements for the degree of MPhil in Law

Lloyd Roughton
University of Oxford, School of Law

July 2021

## ABSTRACT

**Informational Self-Determination in Context: Privacy and Data Protection in the Age of Big Data and Surveillance Capitalism**

Lloyd Roughton

MPhil in Law, July 2021

This thesis focuses on the problem of widespread and sophisticated data collection and processing by private commercial entities, and the threat these practices pose to individual rights and freedoms. This work is directly concerned with European data protection law, and the fundamental rights to privacy and data protection. Particular emphasis will be placed upon the right to informational self-determination, which seeks to ensure individual persons, or 'data subjects', are able to exercise control over their personal data. As will be discussed, this concept is of crucial importance in this context, and is overwhelmingly threatened by the social, economic and technological circumstances of the information age.

The initial discussion will elaborate the problematic nature of the data economy, including the unprecedented scale of this issue and its detrimental consequences. Thereafter, this account will explore fundamental rights, proceeding with the right to privacy, which – despite its renowned importance – is significantly limited and thus unable to effectively respond to a threat of this character. The focus will then turn to data protection, and the need to recognise this right's independent value distinct from privacy. Informational self-determination is essential in this regard, as the importance of data protection is demonstrated through its unique potential to: confer data subject control; and address the overarching power imbalances which currently render such control unfeasible. The success of data protection law relies upon fully developing both of these aspects. Legislative developments have made valid progress with respect to the former, but failed thus far to sufficiently address the latter. Therefore, the final chapter of this thesis will discuss how data protection can evolve to confront the information and power asymmetries of the digital age, in order to create an environment in which individual persons are both protected and empowered.

**Word Count – 28,659**

**ACKNOWLEDGEMENTS**

Firstly, I would like to thank my thesis Supervisor, Dr Justine Pila, for her enlightening oversight and advice during the writing process. Furthermore, I would like to extend my gratitude to the members of the law and emerging technologies discussion group, not only for their critical engagement with my work, but also for offering an enjoyable outlet for thoughtful discussion over the past year.

I would also like to thank the Oxford Human Rights Hub, for allowing me to present my work at their Postgraduate Research Student Conference. A special thanks to Stefan Theil, for offering his insightful feedback at the event.

I must express my deep gratitude to the staff at the University of Glasgow School of Law, for providing me with an invaluable undergraduate education and inspiring me to continue pursuing this area of research.

Finally, I would like to thank all my family and friends who have helped me along the way. In particular my parents, for their constant and unconditional support throughout my entire education, for which I will be forever grateful.

# Table of Contents

# TABLE OF ABBREVIATIONS

| | |
|---|---|
| ECHR | European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5 |
| EU Charter | Charter of Fundamental Rights of the European Union [2007] OJ C303/01 |
| GDPR | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119 |
| Convention 108 | Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108 |
| Data Protection Directive | Directive 95/46/EC 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 [1995] OJ L 0031 |
| TEU | Consolidated version of the Treaty on European Union [2012] OJ C326/01 |
| ECtHR | European Court of Human Rights |
| CJEU | Court of Justice of the European Union |
| GFCC | German Federal Constitutional Court |
| EU | European Union |
| CoE | Council of Europe |
| UK | United Kingdom of Great Britain and Northern Ireland |
| US | United States of America |
| FTC | Federal Trade Commission |
| AG | Attorney General |
| EDPS | European Data Protection Supervisor |
| PIMS | Personal Information Management Systems |

| | |
|---|---|
| AI | Artificial Intelligence |
| IoT | Internet of Things |
| POD | Personal Online Data Store |
| SSI | Self-Sovereign Identity |

# TABLE OF CASES

ECtHR



CJEU

# TABLE OF STATUTES AND OTHER PRIMARY LEGAL SOURCES

# Introduction

> *'There is a wide and growing gap between the condition of individuals de jure and their chances to become individuals de facto – that is, to gain control over their fate and make the choices they truly desire'*
>
> - Zygmunt Bauman, *Liquid Modernity,* 2000[1]

Over the past few decades, we have witnessed the emergence of a uniquely modern threat. Recent technological advancements have afforded us the ability to achieve things we previously thought unimaginable. In particular, the development and rise of computing technology is perhaps the defining feature of human life in the early 21st century. The vast majority of us have become incredibly reliant upon a range of devices – to work, socialise, plan our schedules, travel, read the news, shop – they have become indispensable to the life of a modern day individual. However, as we become increasingly dependent upon these technologies, certain private entities have acquired a unique position with the capacity to collect and process personal data on an almost unimaginable scale. Not only have these corporations enjoyed incredible economic success, but have also amassed a wealth of information pertaining to individuals and the capacity to analyse and deploy this to exert power of a different kind.[2] This is commonly referred to as the rise of 'Big Tech' and has the potential to drastically alter established social relations at the expense of fundamental moral values.

Throughout society, there seems to be a growing general awareness of these developments, yet a widely-acknowledged understanding of the precise nature of this threat

[1] Zygmunt Bauman, *Liquid modernity* (Polity Press 2000) 39.

[2] While important concerns have been raised over governments and public institutions in this context, this thesis is primarily concerned with private and commercial processing of personal data.

has not been achieved. Politicians, lawmakers and other regulatory actors have been grappling with this problem for some time. As a result, privacy and data protection – both as social concepts and legal rights – have attained a new level of importance; and attracted a great deal of attention. The development of the law in response to this emerging issue, in order to protect these fundamental rights and freedoms, is the topic of this thesis. This account focuses on European data protection law, placing particular emphasis on the notion of a 'right to informational self-determination', the right to exercise control over the information pertaining to oneself. As will be discussed, focusing upon this concept is absolutely essential in order for data protection law to offer an effective response to the data economy.

Chapter One is made up of two parts, the first will offer a detailed exploration of the emerging problem this thesis seeks to address; the threat of rapid and sophisticated collection of personal data by private entities in pursuit of commercial ends. This discussion will offer an observation of the technological advancements in the processing of personal data before explaining how these advancements are symptomatic of a fundamental shift in approach towards analysing information, commonly referred to as 'big data', and how certain institutions have sought to utilise the advantages of this for economic gain. This has led to unprecedented asymmetries of power between these institutions and individual persons. Thereafter, the capacity for these developments to have a detrimental impact upon individuals, and wider society, will be discussed.

The second part of Chapter One will explore the concept of privacy, the fundamental right which we have traditionally relied upon in response to threats of this character. As will be discussed, privacy, while of paramount importance, is an inherently

ambiguous concept with almost no scholarly consensus over its precise meaning. Furthermore, recent developments pose an existential threat to the prospect of upholding and maintaining privacy. This thesis will explore these issues in detail, before endorsing a pragmatic approach to privacy, and discussing the assertion that privacy, on its own, may not be enough to offer a solution to our problem.

Chapter Two discusses the relationship between privacy and the relatively new right to data protection. Firstly, however, it will introduce the right to informational self-determination and the fundamental importance such a notion should have regarding the concerns this work has raised. Thereafter, an exploration of the relationship between privacy and data protection will be offered. While some have questioned whether the two should be considered as separate rights, and subsequently cast doubt over the independent recognition of data protection, this thesis will assert that there is an invaluable distinction between the two rights. Furthermore, understanding this distinction is key to unlocking the potential of data protection as a fundamental right. Additionally, this account will make the claim that informational self-determination plays a key role in a strong, effective and independent right to data protection. This chapter will also engage in an analysis of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) case law, focusing on how these courts interpret the relationship between privacy and data protection. It will be submitted that, despite some landmark rulings and valid progress, both courts deploy reasoning which conflates the two rights. Considering the assertions made at the start of the chapter regarding the potential of data protection as a separate right, this is an unfortunate state of affairs.

Following this, Chapter Three will conduct an analysis of The General Data Protection Regulation (GDPR); the most comprehensive and impactful data protection legislation in the world. This discussion will recognise the GDPR's achievements and value, before engaging in a critique of the practical functionality of its provisions. In particular, this will focus on those parts which appear to confer informational self-determination: the rules on consent as a lawful basis for processing; and data subject rights. Overall, this chapter seeks to uncover the symbolic character of the legislation, as – despite important progress – the reality of the complexities and power dynamics of the data economy render the regulation unable to confer true informational self-determination upon data subjects.

Finally, Chapter Four seeks to offer some worthwhile insights regarding the future development of data protection law. The assertions will develop upon the discussion in previous chapters, claiming that – given the current practical unfeasibility of rights of control for data subjects – more focus should be placed upon addressing the overarching and problematic power dynamics which render such rights inadequate. This discussion will initially outline the emerging legal proposals and technological mechanisms which seek to enhance individual data subject control. Thereafter, the focus turns to the future development of the law, advocating for a reconsideration of the foundational principles of data protection to provide the normative force for stronger and more impactful reform. In this regard, this account will specifically focus on the principle of fairness, claiming that a deeper consideration of the conceptual foundations and history of fairness is a worthwhile endeavour, and offering a contribution to such discussions. This chapter will end with a brief outline of emerging proposals for reform, indicating the ways an expanded principle of fairness could contribute to these developments.

A Note on Methodology

Throughout the discussion, this thesis deploys a number of different methodological approaches in each of the four chapters. Hopefully, these different techniques will complement one another in pursuit of a thoughtful and worthwhile discussion. Chapter One adopts a distinctly interdisciplinary lens, drawing upon insights from fields such as philosophy, sociology, social psychology, and computer science in order to elucidate the foundations of the overarching problem we are concerned with, and explore the conceptual basis of the right to privacy.[3] Chapter Two begins by offering some normative claims regarding the relationship between privacy and data protection before conducting an analysis of European data protection law and the jurisprudence of the ECtHR and CJEU, adopting a partially doctrinal perspective in doing so.[4] The methodology for the final two chapters draws upon Khaitan and Steel's work 'Theorising Areas of Law' focusing on 'special jurisprudence;' that is, jurisprudence focusing on theorising 'discrete areas of law.'[5] Chapter Three, in critically analysing the GDPR, applies what these writers label an 'empirical theoretical approach,' which focuses on the causal effects of areas of law.[6] This approach will be discussed further in the initial sections of Chapter Three. Finally, Chapter Four engages in a normative theoretical discussion, seeking to address the underlying

[3] For an in-depth discussion of the relationship between law and other disciplines, see Christopher McCrudden, 'Legal research and the social sciences.(United Kingdom)' 122 Law Quarterly Review 632.

[4] For a discussion of the doctrinal perspective, see Nigel Duncan, 'Defining and describing what we do: doctrinal legal research' 17 Deakin Law Review 83.

[5] Tarunabh Khaitan and Sandy Steel, 'Theorising Areas of Law' (2019) <https://ssrn.com/abstract=3464432> accessed 23 October 2020.

[6] Ibid 19.

principles justifying an area of law,[7] and making the claim that, with regards to data protection law, future reforms should be framed around further pursuit of the principle of fairness.

Credit to Other Scholarly Works

This work draws upon a wide range of sources, however, the works of certain scholars have exercised a heightened level of influence and importance upon this account. In the first chapter, these writers are Viktor Mayer-Schönberger, Kenneth Cukier and Shoshana Zuboff. Furthermore Daniel J. Solove's work heavily influences the conceptual discussions of privacy. In the following chapters, I found the work of a number of data protection scholars particularly useful, including Paul De Hert, Serge Gutwirth and Orla Lynskey. Also, Tatiana Shulga-Morskaya's work 'Protection of personal data through implementation of the right to informational self-determination,' which introduced me to the concept of informational self-determination, must be acknowledged.[8] Finally, a series of articles by Damian Clifford (and others) on fairness in data protection and Lee Bygrave's work, particularly some of the insights in a recent paper on the concept of 'cognitive sovereignty,' offered inspiration and grounding for the normative claims made in the final chapter.[9]

[7] Ibid 21.

[8] Tatiana Shulga Morskaya, 'Protection of Personal Data through Implementation of the Right to Informational Self-Determination: Identifying Opportunities and Pitfalls' (2019 Annual GigaNet Symposium, Berlin, 25 November 2019).

[9] Lee Bygrave, *Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions* (University of Oslo Faculty of Law Research Paper No 2020-35, 2020).

# Chapter One – New Threats to Old Values: Big Data, Surveillance Capitalism and The Concept of Privacy

*'We give people pretty good control over their privacy'*

- Mark Zuckerberg, speaking at Stanford University, 2005[10]

## Introduction

As outlined above, this section will focus on two issues: the emerging problem of big data analysis conducted and deployed by private entities for commercial purposes; and a theoretical discussion of the concept of privacy. The overall purpose of this section is to develop a comprehensive understanding of the complex problem this thesis seeks to address, and demonstrate the unique threat this poses to fundamental societal values; in particular, the right to privacy. As will be discussed, privacy itself has always been a contested and ambiguous notion and, given the scale of the problems faced today, perhaps we may have to look beyond this right in order to protect vulnerable individuals and wider society.

## Big Data and Surveillance Capitalism: A Pervasive, Seismic and Unprecedented Threat

### Pervasive Technologies

In the social world we inhabit today, we are engulfed in an environment of countless information gathering technologies. These devices have become so ubiquitous that it is

[10] Sara Salinas and Anita Balakrishnan, 'Mark Zuckerberg has been talking and apologising about privacy since 2003 - here's a reminder of what he's said' (*CNBC*, 19 December 2018) <https://www.cnbc.com/2018/12/19/facebook-ceo-mark-zuckerberg-privacy-apologies.html> accessed 01 July 2021.

difficult to identify an area of life which entirely evades them; where some aspect of your character, thoughts or actions is not identified and processed.

In the book 'Privacy is Power', Carissa Véliz demonstrates the extent of this intrusion by detailing the catalogue of avenues through which our information can be extracted, in a 'day in the life' of a 21st century person.[11] This begins with mobile phones, which – according to a study by the international data corporation – 79% of us reach for within 15 minutes of waking up.[12] These appliances, attached to the vast majority of us, offer a strikingly powerful and versatile means of collecting data. They have access to our location, conversations, browsing habits, purchases, social media activity, news consumption, and any other activity during which we rely upon an application. A study of Google's Android platform showed that even the most basic functions, such as weather and flashlight apps, deploy intense and sophisticated tracking software.[13]

In what is now referred to as 'the internet of things'[14] (IoT) or 'ubiquitous computing,'[15] rapid advancements in science and engineering have created increasingly tiny processing chips, capable of gathering information. These are inserted into a range of

[11] Carissa Véliz, *Privacy is power : why and how you should take back control of your data* (Bantam Press 2020) 7-26.

[12] IDC, *Always Connected: How Smartphones and Social Keep us Engaged* (An IDC Research Report, Sponsored by Facebook, 2013) 8.

[13] Yael Grauer, 'Staggering variety of clandestine trackers found in popular android apps' (*The Intercept*, 24 November 2017) <https://theintercept.com/2017/11/24/staggering-variety-of-clandestine-trackers-found-in-popular-android-apps/> accessed 7 May 2021.

[14] First referenced in a 1985 speech by Peter T. Lewis, see Chetan Sharma, 'Correcting the IoT History' (*Chetan Sharma Consulting*, 19 June 2020) <http://www.chetansharma.com/correcting-the-iot-history/> accessed 6 May 2021.

[15] For an early articulation, see: Weiser Mark, 'The Computer for the 21st Century' (1991) 265 Scientific American 94.

devices utilised by individuals as we go about our daily lives. Previously mundane appliances – such as watches, doorbells and hoovers[16] – have been upgraded and endowed with data processing capacity while new tech has emerged with these abilities built in, including facial recognition devices[17] and in-home virtual assistants.

Perhaps the most salient aspect of the above description is that it is by no means exhaustive; it does not even begin to scratch the surface. We are living in a culture of data collection on an incomprehensible scale. Jamie Susskind describes this as the 'Increasingly Quantified Society,'[18] whereby human beings now produce more information in a few hours than they did from the beginning of mankind until 2003.[19]

Shifting focus to the future, technology companies are showing no signs of slowing down, as stories emerge of increasingly invasive wearable technology[20] and Elon Musk's recent outlandish claims regarding the brain-machine interface 'Neuralink.'[21] In a book written in 2014, Luciano Floridi describes the impact technology will have on

---

[16] Maggie Astor, 'Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared' *The New York Times* (New York, 25 July 2017) <https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html> accessed 7 June 2021.

[17] Thorin Klosowski, 'Facial Recognition Is Everywhere. Here's What We Can Do About It.' (*Wirecutter*, 15 July 2020) <https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/> accessed 25 April 2021.

[18] Jamie Susskind, *Future politics : living together in a world transformed by tech* (Oxford University Press 2020) 61.

[19] There is some debate over this figure, see Richard E. Susskind and Daniel Susskind, *The future of the professions : how technology will transform the work of human experts* (First edn, Oxford University Press 2015) 161.

[20] Miri Polacheck, '5 companies that want to track your emotions' *Fortune* (New York City, 22 August 2020) <https://fortune.com/2020/08/22/emotion-sensing-tracking-technology-apps/> accessed 1 June 2021.

[21] Patrick McGee, 'Musk-backed Neuralink unveils upgraded brain-implant technology' *Financial Times* (London, 29 August 2020).

human interaction in the environment he terms the 'infosphere.'[22] He predicts, '[in] the near future, the distinction between online and offline will become ever more blurred and then disappear.'[23] While predicting the future of these complex and volatile developments is an almost impossible task, the ambitions of the world's most prominent tech moguls seem to align with this forecast.

These surface level observations of excessive data capture are important, but deeper insight is required in order to come to terms with the problem this work seeks to address. There has been a fundamental shift in the way that certain entities and institutions, particularly private companies with ambitious commercial goals, approach this wealth of personal information. There are two seminal works in this regard, which form the basis of the following discussion, these are Viktor Mayer-Schönberger and Kenneth Cukier's *Big Data,*[24] and *The Age of Surveillance Capitalism*[25] by Shoshana Zuboff.

**A Seismic Shift in Mindset**

'Big data' is a term widely deployed when discussing almost any aspect of the information technology environment. The phrase emerged in the 1990s and, while it is unclear precisely who coined the term, many credit a number of computer scientists working at MIT during this time.[26] Discussions of big data often refer to the characteristics of the datasets

[22] Luciano Floridi, *The 4th revolution : how the infosphere is reshaping human reality* (Oxford University Press 2014).

[23] Ibid 43.

[24] Viktor Mayer-Schönberger and Kenneth Cukier, *Big data : a revolution that will transform how we live, work and think* (New and expanded edn, John Murray 2017).

[25] Shoshana Zuboff, *The age of surveillance capitalism: the fight for a human future at the new frontier of power* (Profile Books 2019).

[26] See Francis X. Diebold, 'On the Origin(s) and Development of the Term 'Big Data'' [2012] SSRN Electronic Journal.

themselves. In an unpublished research note, Douglas Laney highlighted the '3 V's' of big data; volume, variety, and velocity. [27] Subsequent writers have contributed to this discussion, often inserting additional descriptors in an attempt to define the character of complex stores of information.[28]

The present account, however, will focus on big data as denoting a fundamental shift in mindset regarding the way various interested parties approach information, and the implications this will have on society as a whole. Mayer-Schönberger and Cukier offer a compelling analysis of this development, which – according to the authors – consists of three parts: More, Messy and Correlation.

The first aspect describes how statistical analysis has moved away from specific sampling as the dominant method, to gathering as much information as possible, represented by the simple equation 'n=all.'[29] This new perspective affords new freedom to explore, approach from different angles, and identify specific aspects of the data, all without the risk of blurriness or missing out on key insights – a risk inherent to the sampling methodology.[30] As stated by the authors, 'reaching for a random sample in the age of big data is like clutching at a horse whip in the era of the motor car.'[31] The second part, the messiness of big data, describes how we come to accept inexactitude as datasets grow in

---

[27] Ibid 4.

[28] Rob Kitchin and Gavin McArdle, 'What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets' (2016) 3 Big data & society.

[29] Mayer-Schönberger and Cukier (n 24) 26.

[30] Ibid 29-30.

[31] Ibid 31.

size. In the exercise of collecting ever larger amounts of data, the likelihood of inaccuracy increases but the value of the new insights offset the impact of any errors.[32] In the era of big data, if we learn to live with messiness then 'more trumps better' and 'we open a window into an untapped universe of insights.'[33] The third and final change is that, where we once upheld the importance of causation, we have shifted our focus to correlation.[34] We have moved away from identifying the cause of a phenomenon, to using algorithms to identify correlations in vast documents in order to, for example, decide on targeted ads for a specific user. We do not fully understand the insights offered by this process, but that does not matter, 'knowing what, not why, is good enough.'[35]

These new approaches to information are linked to the concept of 'Datafiation.' This denotes the process of placing a phenomenon 'into a quantified format so that it can be tabulated and analysed'[36] and this allows one to extract insights and value from information which nobody previously thought held any use at all. For instance, a vast dataset can be created of individuals who have searched online for 'home mortgage' and all their subsequent searches. Analysis of this information can reveal crucial insights regarding when those same individuals will seek to purchase home insurance, furnishings, and garden accessories.[37]

---

[32] Ibid 32-34.

[33] Ibid 47.

[34] Ibid 50.

[35] Ibid 52.

[36] Ibid 78.

[37] José van Dijck, 'Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology' (2014) 12 Surveillance & Society 197, 201.

It must be acknowledged that big data has great potential to make important and valuable contributions to society, and indeed already has in areas such as medicine,[38] education,[39] and combatting climate change.[40] The logic of big data itself is not inherently problematic, but the thesis comes with a warning, 'wielded unwisely, it can become an instrument of the powerful.'[41] The implication here is that if these abilities fall into the wrong hands – or rather the hands of those with the wrong motivations – the potential for negative consequences is just as great. Unfortunately, the value of datafication was discovered by a little-known silicon valley start-up named Google, in the aftermath of the dotcom crash and under intense pressure from venture capitalist investors to start making profit, and fast.

This denotes the beginning of the phenomenon Zuboff describes as *surveillance capitalism.* This groundbreaking work offers an incredibly comprehensive account, the current analysis will simply seek to establish some of the integral concepts as it takes up such a central role in this thesis. The story starts with the employees at Google, and '*the discovery of behavioural surplus.*'[42] Initially, any information gleaned from user activity would be fed back into the system for the sole purpose of improving user experience, in '*the behavioural value reinvestment cycle.*'[43] This all changed with the realisation that there

[38] Ziad Obermeyer and Ezekiel J. Emanuel, 'Predicting the Future — Big Data, Machine Learning, and Clinical Medicine' (2016) 375 The New England journal of medicine 1216.
[39] Ben Williamson, *Big data in education : the digital future of learning, policy and practice* (SAGE Publications Ltd. 2017).

[40] Zhihua Zhang and Jianping Li, *Big data mining for climate change* (Elsevier 2020).

[41] Mayer-Schönberger and Cukier (n 24) 151.

[42] Zuboff (n 25) 74.

[43] Ibid 69.

were large quantities of personal data – previously discarded as 'data exhaust' – which can be used 'to read users' minds for the purposes of matching ads to their interests.'[44] The tech entrepreneurs had discovered the wonders of datafication and had the realisation that they were uniquely placed to reap the benefits. They subsequently set out to collect as much personal data they could in as many ways as possible; Zuboff calls this '*the extraction imperative.*'[45] Consider the wealth of technologies we now find ourselves surrounded by, as explored in the previous section. These are not the inevitable products of technological progress, but rather the result of ambitious corporations seeking to utilise this data in pursuit of commercial ends.

Against the backdrop of unfettered capitalist ideologies procured in the US and much of the western world in the late 20th century, the discovery of behavioural surplus marked the beginning of the economic ideology of surveillance capitalism.

Surveillance Capitalism (noun):

1. A new economic order that claims human experience as a free raw material for hidden commercial practices of extraction, prediction, and sales.
2. A parasitic economic logic in which the production of goods and services is subordinated to a new global architecture of behavioural modification.[46]

While Zuboff's work is the most prominent account, the way information processing has become dominated by corporate entities has been widely observed. Lyon, detailing the

---

[44] Ibid 78.

[45] Ibid 87.

[46] Ibid (preface).

impact of big data upon surveillance practices notes that corporate strategy has become the 'decisively significant factor' and that big data is now more commonly associated with economic worth, as opposed to its other uses.[47] In an account similar to Zuboff's, West demonstrates that the allure and appeal of greater connected social communities through social media led to the rise of 'data capitalism,' built upon commoditisation of personal information.[48]

**Unprecedented information and power asymmetries**

It has become commonplace to refer to data as 'the new oil,'[49] a valid comparison as data went from a previously untapped resource to a lucrative commodity, creating new sources of revenue for those who collect it and accelerating the rise of a new industry. The comparison ends, however, when we consider that the power acquired by those who process personal information is unprecedented. Big tech is inherently different in character to big oil, or any other traditional industrial corporation.

Zuboff explains that 'the division of learning in society'[50] is central to these new power dynamics. This builds upon Emile Durkheim's concept of the division of labour,[51]

[47] David Lyon, 'Surveillance, Snowden, and Big Data: Capacities, consequences, critique' (2014) 1 Big data & society 5.

[48] Sarah Myers West, 'Data Capitalism: Redefining the Logics of Surveillance and Privacy' (2019) 58 Business & society 20.

[49] British mathematician Clive Humby is credited with coining this phrase, see Charles Arthur, 'Tech giants may be huge, but nothing matches big data' *The Guardian* (London, 23 August 2013) 6; see also 'The world's most valuable resource is no longer oil, but data' *The Economist* (London, 6 May 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> .

[50] Zuboff (n 25) 184.

[51] Emile Durkheim and Steven Lukes, *Durkheim: The Division of Labour in Society* (2nd edn, Palgrave Macmillan 2013).

the principle which structured social systems and maintained reciprocity in modern industrial societies. According to Durkheim, the greatest threat to this structure is extreme social inequality and accompanying asymmetries of power, preventing the people from contesting and confronting power. For Zuboff, the 'privatisation of the division of learning'[52] mirrors these developments. Private entities who engage in the collection of data have acquired such a wealth of knowledge and information that they have created an unprecedented asymmetry of power against those whose data they collect.

The lack of reciprocity is a theme throughout, 20th century production companies relied upon the masses as workers and consumers. In the data economy there is no such relationship, we may view the processing of data as a transaction in return for free online services. For surveillance capitalists, however, this is merely a means of acquiring behavioural surplus for analysis, the real transaction is the sale of prediction products. This 'marketplace in behavioural futures'[53] allows Surveillance Capitalists to 'impose a new kind of control upon individuals, populations and whole societies.'[54]

Let us briefly consider the work of Michel Foucault, perhaps the preeminent philosopher on the subject of power. Lecturing at the Collège de France in 1975, Foucault contests the perception of power as 'a phenomenon of mass and homogenous domination.'[55] Instead, he deploys and analogy to electricity, in modern societies 'power

[52] Zuboff (n 25) 189.

[53] Ibid 96.

[54] Ibid 191.

[55] Michel Foucault, *'Society Must Be Defended' Lectures at the Collège de France 1975-76* (Mauro Bertani and Alessandro Fontana eds, David Macey tr, Picador, New York 2003) 29.

is something that circulates through individuals not something that is applied to them.'[56] With surveillance capitalism, the exponential acquisition of personal information creates an entirely new and disconcertingly effective means of exercising power over people. The energy is drained from Foucault's metaphorical circuit and the power of specific institutions is amplified. One of Foucault's central critiques of modernity described the way we are conditioned and disciplined in certain 'enclosures,' disciplinary institutions we inhabit at certain points in our lives; such as the school, hospital, or military.[57] The power asserted upon individuals today, however, is becoming increasingly reminiscent of Deleuze's societies of control, whereby computational advancements create a societal structure in which power is asserted in a continuous and omnipresent manner.[58]

The Detrimental Impact on Individuals and Society

Through sophisticated data collection practices surveillance capitalists solidify unique positions of power, this enables them to exercise control over individual persons. The following discussion identifies three different ways that corporate big data practices have a negative impact on people in society – the chilling effect of surveillance; the control effect; and the capacity for discrimination, unwarranted bias and unfair treatment.

The 'chilling effect' describes the way persons alter their behaviour when they feel under surveillance. The concept originated in discussions of US first amendment

[56] Ibid.

[57] Michel Foucault, *Discipline and punish: the birth of the prison* (Penguin 2019) 95-159.

[58] Gilles Deleuze, 'Postscript on the Societies of Control' (1992) 59 The MIT Press 3; see also Zuboff's discussion of 'big other': Zuboff (n 25) 376-397.

jurisprudence and Frederick Schauer is credited with defining the concept, whereby individuals are 'deterred' from activities they would otherwise participate in due to 'invidious' surveillance practices.[59] Cohen discusses the chilling effect in the context of informational privacy, 'pervasive monitoring of every first move or false start will, at the margin, incline choices towards the bland and mainstream.'[60] A study of Wikipedia searches following the Snowden revelations supports the chilling effect theory, demonstrating a significant decline in traffic towards 'privacy-sensitive' articles following the 2013 Snowden revelations on mass internet surveillance.[61] While 20th century observations of the chilling effect, and indeed the Snowden revelations, were focused on government surveillance, today the threat of corporate practices having the same, or even greater, impact is deeply concerning.[62] There is a general awareness throughout society today that our data is being collected on a large scale, we are 'conscious of our role as subjects of these critiques,'[63] and yet a more detailed understanding of the use of this data is not commonplace. Such a cautious mindset could lead people to self-censor their behaviour, through fear of judgment, consequences or manipulation. This has the potential to have a severe and wide ranging impact on individual autonomy, creating a 'nightmare scenario… turning us into quivering, neurotic beings living in a psychologically oppressive world… constantly aware that our every smallest move is being charted,

[59] Frederick Schauer, 'Fear, Risk and the First Amendment: Unraveling the Chilling Effect' (1978) 58 Boston University Law Review 685, 689-690.

[60] Julie E. Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 Stanford Law Review 1373, 1425-1426.

[61] Jonathon Penney, 'Chilling Effects: Online Surveillance and Wikipedia Use' (2016) 31 Berkeley Technology Law Journal 117.

[62] See, Jonathan Shaw, 'The Watchers: Assaults on Privacy in America' (*Harvard Magazine*, January 2017) <https://www.harvardmagazine.com/2017/01/the-watchers> accessed 13 April 2021.

[63] Jay Stanley, 'The Potential Chilling Effects of Big Data' (*American Civil Liberties Union*, 30 April 2012) <https://www.aclu.org/blog/privacy-technology/consumer-privacy/potential-chilling-effects-big-data> accessed 13 April 2021.

measured, and evaluated against the like actions of millions of other people,'[64] and then utilised to judge us in ways we are unable to understand or predict.

While mere awareness of surveillance can have a detrimental impact on individuals, further concerns arise regarding the way big data actors engage in a 'unique interaction with a specific individual.'[65] Benefitting from 'personalised digital interfaces' data collectors can interact with individual users and exert an astounding degree of control upon their behaviour, enabled by insights gleaned from sophisticated analysis of previously collected personal data.[66] These control capabilities are perhaps the most disconcerting aspect of surveillance capitalism, and constitute an important focal point of Zuboff's work. The author traces how surveillance capitalists moved into *'the reality business'* by adopting the *'prediction imperative,'* seeking to develop increasingly intricate and sophisticated prediction products. Their operations expanded to accommodate both economies of *scope* and *action*. The former refers to the development of new supply routes for data which are more predictive and intimate; aimed at individual personalities, needs and emotions. The latter explains the ways they seek to 'nudge, tune, herd and manipulate' human behaviour. The entire development is summarised as the *'21st century means of behavioural modification'* the aim of which is to 'produce behaviour that reliably, definitely and certainly leads to desired commercial ends.'[67]

[64] Ibid.

[65] Tal Z. Zarsky, 'Incompatible: The GDPR in the Age of Big Data.(General Data Protection Regulation)' (2017) 47 Seton Hall Law Review 995, 1000.

[66] Ibid.

[67] Zuboff (n 25) 197-202.

Many scholars have offered detailed observations of these unsettling abilities. Kerr & Eale describe how techniques of prediction, pre-emption and presumption 'enable a universalizable strategy of preemptive social decisionmaking' on the part of the data collectors, which is 'antithetical' to fundamental values.[68] Yeung argues that the idea of 'nudging' – subtly pushing data subjects towards certain choices – may not be fully reflective of the power of these practices. She applies the label 'hypernudge', as 'due to their networked, continuously updated, dynamic and pervasive nature,' they exert an extremely complex and sophisticated level of control over individuals.[69]

Finally, we turn to the potential for commercial deployment of large datasets to lead to discrimination and unfair treatment; often towards already disadvantaged groups. According to the big data mindset, we collect as much data as possible, learn to live with inexactitude and primarily focus on correlation at the expense of causation. Despite the benefits this may afford, large datasets are often 'encoded with human prejudice, misunderstanding and bias'[70] on the part of those who design them. When these misconceptions are extrapolated out into large datasets which make significant and impactful decisions regarding individual persons, unfair treatment is imposed on a large scale.[71] Especially when those running these systems are only concerned with efficiency

[68] Ian Kerr and Jessica Earle, 'Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy' (*Stanford Law Review*, September 2013) <https://www.stanfordlawreview.org/online/privacy-and-big-data-prediction-preemption-presumption/> accessed 01 February 2021.

[69] Karen Yeung, ''Hypernudge': Big Data as a mode of regulation by design' (2017) 20 Information, communication & society 118.

[70] Cathy O'Neil, *Weapons of math destruction : how big data increases inequality and threatens democracy* (Penguin Books 2017) 3.

[71] For a discussion of the concerns with big data's underlying principles and the potential 'traps' this may lead to, see: Tim Harford, 'Big data: are we making a big mistake?' *Financial Times* (London, 28 March 2014) <https://www.ft.com/content/21a6e7d8-b479-11e3-a09a-00144feabdc0> accessed 16 April 2021.

and profit maximisation. The mathematician Cathy O'Neill labels these algorithms 'Weapons of Math Destruction' and describes how these systems rank and judge us, based on vast and detailed stores of personal data, at critical junctures in our lives.[72] Examples include automated hiring systems which screen out candidates based on race or mental health status,[73] predictive algorithms for policing which encourage officers to intensify their efforts on specific socially deprived areas (often with high populations of ethnic minorities),[74] and 'arbitrary [and] unaccountable' e-scores which determine credit scores and deny people loans.[75] These observations support Lyon's concept of 'surveillance as social sorting' whereby deployment of these statistical models to map and predict human behaviour facilitates 'a powerful means of creating and enforcing long-term social differences.'[76] The issue is compounded when we consider that those running these systems often do not fully understand the complexity of them, this complexity creates distance from the decision itself, enabling otherwise illegal discrimination to become perfunctory and routine.[77] Furthermore, an empirical study uncovered that those who engage with big data analytics are met with significant barriers even if they make an effort to practice 'fair data-mining,' such as 'technical difficulties, conceptual challenges, human bias and shortcomings of legislation.'[78]

---

[72] O'Neil (n 70).

[73] Ibid 107-113.

[74] Ibid 87.

[75] Ibid 141-143.

[76] David Lyon, 'Surveillance as social sorting: computer codes and mobile bodies' in David Lyon (ed), *Surveillance as social sorting: privacy, risk and discrimination* (Taylor & Francis Group 2002).

[77] See discussion of the link between 'statistical surveillance' and 'statistical discrimination' in: Oscar H Gandy Jr, 'Statistical surveillance: Remote sensing in the digital age' in K Ball, K Haggerty and David Lyon (eds), *Routledge Handbook of Surveillance Studies* (London, Routledge 2012) 130.

[78] Maddalena Favaretto, Eva De Clercq and Bernice Simone Elger, 'Big Data and discrimination: perils, promises and solutions. A systematic review.(Research)(Report)' (2019) 6 Journal of Big Data 23.

## A Fundamental yet Ambiguous Value

The question of how to respond to these threats to protect individuals and established moral values – a dilemma faced by lawmakers, advocates and wider society – is a deeply unenviable task. Throughout history, although particularly in modern Western societies – when faced by behaviours or actions which posed similar challenges, we have relied upon the fundamental, yet somewhat illusive, concept of privacy. While these emerging practices present a far more advanced and sophisticated threat than those we have encountered previously, for many people privacy remains the 'preeminent mobilising concept'[79] for combatting the potential harms introduced by these developments. The concept has acquired the status of a fundamental right in many jurisdictions, enshrined in a number of international human rights instruments.

Despite privacy's fundamental importance and widely-recognised intuitive value, the concept is deeply contested and inherently ambiguous. Privacy is commonly associated with protection – protecting some aspect of ourselves as human beings – but what exactly is it that privacy seeks to protect? how can we explain and justify its meaning and existence as a value of importance? When seeking to develop a greater understanding of privacy, one is met with an 'exasperatingly vague and evanescent'[80] discourse; 'there is no single definition or analysis or meaning of the term.'[81] Western scholars appear to have developed

[79] Lyon (n 76) 10.

[80] Arthur R. Miller, *The assault on privacy : computers, data banks, and dossiers* (University of Michigan Press 1971) 25.

[81] Judith DeCew, 'Privacy' (*The Stanford Encyclopedia of Philosophy*, Spring 2018 Edition) <https://plato.stanford.edu/archives/spr2018/entries/privacy/> accessed 2 February 2021.

an obsession with finding a conceptual core to provide the foundations for privacy and achieve a more settled understanding. Although these conflicting accounts have created ambiguity, the insights put forward are of great value in elaborating the different aspects of privacy's character. This work will proceed by outlining some of the most prominent theories, not in an attempt to offer a complete picture (as doing so is substantially outside of the scope of this work) but rather to demonstrate the range and variation of perspectives across the most influential conceptions.

Warren and Brandeis' 1890 Harvard Law Review article 'The Right to Privacy' is credited as the first systematic account of privacy as a legal right.[82] In response to the invention of instantaneous photography and the prevalence of yellow journalism, the authors embark upon a passionate defence of the individual 'right to be let alone;' the 'protection afforded to thoughts, sentiments and emotions' from unjustified interference or publication.[83] The account demonstrated that the existing American common law protects such a right, which can be invoked to protect individual privacy and is grounded upon the principle of 'inviolate personality.'[84] The article continues to be held in the highest regard, often described as the most influential law review article of all time. However, it has been criticised as offering a conception of privacy that is too broad or vague. Perhaps because the authors do not appear to offer a unifying conceptual account of privacy, but rather to advocate for its recognition in the law. A prominent critique of Warren and Brandeis work is offered by Prosser, who claimed that – rather than being an independent value – privacy is in fact a combination of four tourts: intrusion into the plaintiff's seclusion or solitude;

[82] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.

[83] Ibid 205.

[84] Ibid.

public disclosure of embarrassing facts; publicity which placed the plaintiff into a 'false light'; and appropriation of the plaintiff's name or likeness.[85] A few years later, Bloustein responded to Prosser, defending Warren and Brandeis' article and the value of identifying the central value of privacy.[86] While Bloustein claims that Warren and Brandeis failed to develop a positive definition of privacy, he credits their identification of the importance of 'inviolate personality' and develops the case for this as the unifying value of privacy. He proceeds, asserting a conception of privacy as human dignity, which defines one's essence as a human being, including individual dignity and integrity, personal autonomy and independence. Each of the invasions identified by Prosser are affronts to this human dignity, and so that is the unifying value of privacy.

This scholarly quest to identify the central meaning of privacy can be observed elsewhere, with a range of proposals and interpretations put forward. Other accounts include 'limited access to the self' – an early articulation of this view describes privacy as 'the right to decide how much knowledge of personal thought and feeling… private doings and affairs… the public at large shall have.'[87] Another perspective is privacy as 'intimacy', a contemporary account of this is offered by Inness, who claims that intrusions characterised as privacy are united by 'the common denominator of intimacy.'[88]

[85] William L. Prosser, 'Privacy' (1960) 48 California Law Review 383, 389.

[86] Edward J. Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 New York University Law Review 962.

[87] Edwin Lawrence Godkin, 'The Rights of the Citizen, IV—To His Own Reputation' *Scribner's Magazine* (New York, July-Dec 1890) 65.

[88] Julie C. Inness, *Privacy, intimacy, and isolation* (Oxford University Press 1992) 139.

The varying conceptions of privacy all link and overlap, it has been observed that 'limited access to the self' is connected to the 'right to be let alone,'[89] and Warren and Brandeis' account is credited with providing the basis for a number of conceptions.[90] While many of the accounts are valuable, as they offer valid and in-depth insights into the different aspects of privacy, no conception has afforded a unifying understanding which can provide the basis for a coherent consensus.

**The Existential Threat to Privacy**

While privacy has come under threat due to advancements in technology before (Warren and Brandeis' piece was inspired by the instant photography and newspaper gossip) the onslaught privacy faces today, at the hands of surveillance capitalism, poses an existential threat to its status as a cherished and valued social norm.

In the 1964 book 'The Naked Society', Vance Packard observes the emerging trend of businesses commercialising personal information for economic gain. He observes, 'the expectation that one has a right to be let alone—the whole idea that privacy is a right worth cherishing—seems to be evaporating among large segments of our population.'[91] Any observation of corporate big data practices necessarily raises deep concerns regarding the threat to privacy, no matter what conception of privacy one may subscribe to. In a world where private institutions have the capacity to process data to an unprecedented extent – affording them the ability to exercise sophisticated control over individuals and populations

[89] Solove describes the former as a 'more sophisticated' version of the latter: Daniel Solove, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087, 1102.

[90] DeCew (n 81).

[91] Vance Packard, *The naked society* (Penguin 1966) 12.

– how can we rely on a concept such as privacy to protect values such as dignity, intimacy or seclusion. As the authors of 'Big Data' observe, in a section entitled 'paralyzing privacy', 'the problem has been transformed.'[92]

An image central to most discussions of privacy is the spatial metaphor of the private and public spheres, as 'privacy is frequently employed to describe a zone demarcated as private.'[93] But as these practices continue to demand a growing influence on our daily lives, the distinction between the two spheres becomes blurred. Once sacred facts about our lives are now immediately available to these powerful institutions, and this has taken place 'through small concessions that have mounted up over time.'[94] Most of our engagements with privacy take place through a perverse economic transaction, whereby privacy rights are reduced to an economic commodity. As Pasquale observes, privacy is treated as 'a product that individuals have varying preferences for and purchase accordingly,'[95] based on the fallacy that individual persons engage rationally with complex consent notices before opting to use certain internet services.

There exists a deeply concerning yet wide ranging narrative that privacy is an out-dated value, no longer relevant for the computerised information age, as 'countless books and articles have heralded the 'end', 'death', and 'destruction' of privacy.'[96] In 2010, Mark

[92] Mayer-Schönberger and Cukier (n 24) 153.

[93] Raymond Wacks, *Privacy : a very short introduction* (Second edn, Oxford University Press 2015) 34-35.

[94] Alex Preston, 'The death of privacy' *The Guardian* (London, 3 August 2014) <https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston> accessed 30 February 2021.

[95] Frank A. Pasquale, 'Privacy, antitrust, and power' (2013) 20 George Mason Law Review 1009, 1016.

[96] Daniel Solove, 'The End of Privacy?' (2008) 299 Scientific American 100, 103.; for an example, see James B. Rule, *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience* (Oxford University Press 2009).

Zuckerberg suggested privacy is no longer a social norm.[97] Furthermore, in a campaign promoting government surveillance, the UK Government adopted the slogan 'if you've got nothing to hide, you've got nothing to fear,'[98] an unsettling position which undermines the fundamental importance of privacy in order to justify intrusive state surveillance.

**Moving Forward: Pragmatism, Control over Personal Information and Looking Beyond Privacy**

One of the most compelling accounts of the concept of privacy is advanced by Daniel Solove in the article 'Conceptualizing Privacy'.[99] A large part of this work is dedicated to a critique of the varying conceptions of privacy which, according to Solove, adopt the 'traditional method' of identifying a 'common set of necessary and sufficient elements that single out privacy as unique' and formulating a conception based on these elements.[100] Given the lack of unifying consensus achieved by this endeavour, he proposes an alternative approach based on Wittgenstein's notion of 'family resemblances.' According to Wittgenstein, certain concepts do not need to be defined by reference to a common denominator. Alternatively, each instance of a concept can be said to draw from a pool of similar characteristics.

---

[97] Bobbie Johnson, 'Privacy no longer a social norm, says Facebook founder' *The Guardian* (London, 11 January 2010) <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy> accessed 29/02/2021.

[98] Daniel Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 The San Diego Law Review 745, 748.

[99] Solove, 'Conceptualizing Privacy' (n 89).

[100] Ibid 1095.

Wittgenstein focuses on the philosophy of natural language: words or phrases are not defined by one unifying concept, but rather draw upon a range of possible uses and the exact meaning in a particular instance depends upon the context in which it is deployed. This collection of possible meanings consists of 'a complicated network of similarities overlapping and criss-crossing: sometimes overall similarities, sometimes similarities of detail.'[101] For example, the word 'game' could represent a trivial and fun activity – like a board game or a card game – or a much more professional and prestigious event, such as the Olympic games. The proper meaning of a term often depends entirely on the context, and the same pragmatic approach should be used to define privacy. As Solove acknowledges that 'each of the conceptions of privacy… elaborates upon certain dimensions of privacy and contains countless insights,' it can be inferred that these accounts represent the network of possible meanings; it is merely the attempt to identify one of them as the unifying concept which is flawed, as it 'results in either a reductive or an overly broad account of privacy.'[102] This, I believe, offers the most valid approach to conceptualizing privacy and solves the problem created by the search for a single overall concept, which has left the discourse in a state of 'chaos.'[103] It is also not too broad a conception, as we have the various accounts of privacy available to us – of dignity, intimacy, seclusion, secrecy and so on – as possible characteristics to draw upon in different contexts.

Therefore, if the meaning of 'invasion of privacy' can draw upon any of the different facets of privacy – to varying extents in different circumstances – how do we

[101] Ludwig Wittgenstein, *Philosophical Investigations* (G.E.M Anscombe tr, Basil Blackwell 1958), §66.

[102] Solove, 'Conceptualizing Privacy' (n 89) 1124.

[103] Inness (n 88) 3.

understand such a term in the context of the developments with which this work is concerned? One particularly interesting and relevant conception of privacy for our purposes here is privacy as control over personal information. In 1968, offering his perspective in the book *Privacy and Freedom,* Alan F. Westin asserted that:

> Privacy is the claim of individuals, groups and institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others.[104]

While Westin's account is the most prominent and widely cited example of privacy as control over personal information, many other scholars have put forward a similar view.[105] This view defines privacy as the ability to exercise control over the information pertaining to oneself, this encompasses all personal information, and is infringed when we are prevented from exercising such control.

This conception of privacy is immediately appealing, and worthy to note here, as it is commonly cited as a developed understanding of privacy capable of responding to the challenges of modern data processing. However, concerns have been raised over extending privacy to such a broad notion, as this detaches it from its conceptual foundations and 'rich history,' potentially leading to 'the domination of an eroded concept of privacy.'[106] I am inclined to agree with this view, while I endorse Solove's pragmatic approach, privacy should be attached to recognised but context dependent values – such as dignity, seclusion, and secrecy – and concerned with maintaining a private and public sphere. The wider

[104] Alan F. Westin, *Privacy and freedom* (1st edn, Atheneum 1968) 7.

[105] For a summary of these accounts, see Solove, 'Conceptualizing Privacy' (n 89) 1110.

[106] Serge Gutwirth, *Privacy and the information age* (Rowman & Littlefield 2002) 2.

challenge of controlling personal information should be the primary concern of a new, distinct and broader right; namely, the right to the protection of personal data. This assertion will be explored extensively in the next chapter, which we turn to following a brief summary of this chapter.

Summary

This chapter has sought to, firstly, offer a comprehensive understanding of the problematic impact of the combination of big data and surveillance capitalism. The development of innovative and useful technologies has been embraced by almost all of us, but this convenience comes at a price.[107] Wilfully transferring our data to powerful corporations has enabled them to construct regimes of private surveillance, exercise sophisticated and effective control over individuals, and compound social inequalities through unfair and biased algorithms.

The inherent ambiguity of privacy perhaps explains why society has thus far been so woefully unequipped to respond to these developments. As a result, surveillance capitalism seems to have almost entirely undermined such a fundamental right. While defending Solove's approach, it is asserted that extending privacy to an overly broad notion such as 'control over personal information' is not to be advised. A legal response to the detrimental consequences of the data economy requires the emergence of a new right, directly concerned with the use of these advanced technologies, to work alongside privacy.

[107] Tim Wu, 'The Tyranny of Convenience' *The New York Times* (New York City, 16 February 2018) <https://www.nytimes.com/2018/02/16/opinion/sunday/tyranny-convenience.html> accessed 09 December 2020.

Fortunately, in Europe, this has already occurred, with the emergence of the right to the protection of personal data.

# Chapter Two – Informational Self-Determination and the Relationship Between Privacy and Data Protection

*'Political, social and economic changes entail the recognition of new rights'*

- Warren and Brandeis, *The Right to Privacy*, 1890[108]

## Introduction

Chapter One established and explored the problem this thesis seeks to address, and offered an initial overview of the concept of privacy, the long established right which we would traditionally deploy in response to such concerns. However, it was acknowledged that privacy may be unable to offer sufficient protection for individuals from the formidable threat of surveillance capitalism.

The purpose of this chapter is to, firstly, establish the right to informational self-determination and assert the fundamental importance such a concept should have in response to the problems we are concerned with here. Thereafter this section will discuss the relatively modern right to data protection, which emerged in response to advancements in information processing, and its relationship with the well-established right to privacy. While some questions have been raised regarding the purpose of data protection, this account will fully support the view that this right has unique value outside of privacy, and – if developed correctly – has great potential to offer a strong regulatory response to the detrimental effects of corporate big data practices. Furthermore, through this discussion we will be able to observe the key role played by informational self-determination in an effective independent right to the protection of personal data.

[108] Warren and Brandeis (n 82) 193.

Following this, the role of privacy and data protection in European data protection law will be analysed, beginning with an outline of the relevant legislation and human rights instruments. Thereafter, this thesis will undertake an analysis of the jurisprudence of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU). This section, adopting a doctrinal perspective, will focus on the interpretation of the relationship between privacy and data protection in the case law. This account will seek to demonstrate that, while some valuable progress has been made, both courts conflate the rights of privacy and data protection. This reasoning is deeply unfortunate, as this weakens the standing of data protection as a fundamental right.

Informational Self-Determination and the Emergence of Data Protection

In the previous chapter, Westin's notion of privacy as control over-personal information was discussed. In Europe, a similar right, pertaining to controlling the information about oneself, emerged: the right to informational self-determination. The earliest articulation of this comes from a 1983 decision by the German Federal Constitutional Court (GFCC), in response to a government plan to conduct an extensive population census. The court recognised a right to informational self-determination (Informationelle Selbstbestimmung), defined as:

> The power of individuals to make their own decisions as regards the disclosure and use of their personal data, [while] restrictions of this right are permissible only in the case of overriding general public interest. [109]

[109] Judgment of 15 December 1983, 1 BvR 209/83 ECLI:DE:BVerfG:1983:rs198312151bvr020983.

This concept is of paramount importance and focus throughout this thesis. This is because, at a very fundamental level, this ability to control personal information is precisely what has been taken away from us. This is an affront to our modern post-enlightenment understanding of the individual as a rational and autonomous human being. Returning to Zuboff, 'we experience both the right and requirement to choose our own lives. No longer content to be anonymous members of the mass, we feel entitled to self-determination, an obvious truth to us… This mentality is an extraordinary achievement of the human spirit.'[110] The unprecedented and massive collection of personal data to fuel regimes of private surveillance, engaging in practices of control and unfair treatment, exhibits a lack of respect for the moral agency of individual persons. The concept of informational self-determination goes to the very core of this problem, the unjust appropriation at the heart of surveillance capitalism.

The ruling of the German court is particularly interesting because of the conceptual grounding offered by the court as the basis for this right. The right was justified upon 'the fundamental values of 'human dignity' and 'self-development'[111] enshrined in German Basic Law,[112] and the court 'traced the foundations… to the free-development of one's personality'[113] in the constitution. As there is no specific right to privacy in the German

[110] Zuboff (n 25) 35.

[111] Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009) 46.

[112] Germany: Basic Law for the Federal Republic of Germany [Germany], 23 May 1949, arts 1(1), 2(1).

[113] Rouvroy and Poullet (n 111) 49.

constitution, the court did not associate this rights-based enhanced control over personal data with the right to privacy.

The late 20th century also saw the emergence of data protection throughout Europe, this began in the 1970s with German and Swedish legislation responding to concerns over government control through computerised national data banks, but has since developed and now concerns both public and private data collection.[114] As will be disused further below, data protection was eventually recognised as a fundamental right in the EU Charter.

While the ruling of the German Court is widely cited in discussions surrounding data protection, informational self-determination and data protection are not identical. Indeed, German proposals to formulate Article 8 of the EU Charter as such were struck down.[115] The emergence of data protection alongside privacy raises a number of questions which the following section will seek to answer, such as: why was data protection recognised as a separate right outside of privacy? How are the two rights respectively defined? What is their relationship with one another? And how should informational self-determination factor into this?

[114] For a discussion of the development of data protection law, see Viktor Mayer-Schönberger, 'Generational development of data protection in Europe' in *Technology and privacy: the new landscape* (MIT Press 1997).

[115] Herke Kranenborg, 'Protection of Personal Data' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing 2014) 229; see also, Draft Charter of the Fundamental Rights of the European Union (05 May 2000) https://www.europarl.europa.eu/charter/activities/docs/pdf/convent28_en.pdf.

Firstly, it must be acknowledged that some scholars view the recognition of data protection, as separate from privacy, as a mistake. Because data protection 'seems to be indebted to the central objective of the right to privacy,' it is therefore 'perceived as a late privacy spin off' and many consider the two rights to be 'interchangeable.'[116] Rouvroy and Poullet describe the development of privacy culminating in an understanding of privacy as informational self-determination and, in doing so, describe data protection law as merely a tool to protect privacy.[117] This sort of approach treats informational self-determination as a 'conceptual link'[118] between privacy and data protection which merges the two concepts, as 'some assume data protection ensures informational self-determination, and subsequently argue that privacy is in fact a right to informational self-determination and thus equals data protection.'[119] Furthermore, this viewpoint is supported by Terwangne, describing informational self-determination as 'another dimension of privacy,'[120] and the Council of Europe, which identifies it as 'a new concept of privacy' in response to 'the rise of the information society'[121] in its handbook on data protection law.

[116] Serge Gutwirth and Paul De Hert, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009) 4.

[117] Rouvroy and Poullet (n 111) 70.

[118] Kranenborg (n 115) 229.

[119] Ibid

[120] Cécile de Terwangne, 'The right to be forgotten and the informational autonomy in the digital environment' in A Ghezzi, Â.G Pereira and L Vesnić-Alujević (eds), *The Ethics of Memory in a Digital Age Palgrave Macmillan Memory Studies* (Palgrave Macmillan 2013) 4.

[121] Council of Europe, *Handbook on European data protection law 2018 edition* (Luxembourg : Publications Office 2018) 18.

However, it is submitted that the above perspective is mistaken and unfortunate. This thesis supports the view that the emergence of data protection as a separate right was a valuable development. Furthermore, there is a distinct conceptual distinction between privacy and data protection, and data protection can work outside of privacy to empower and protect individuals in response to the threats posed by modern data processing practices.

To understand the difference between privacy and data protection, we can begin by considering the foundations of the latter. Data protection laws were first implemented, then subsequently developed, in response to rapidly advancing forms of information processing which presented a new threat to individuals through the use of data which would not typically be considered 'private'. Previous interferences with 'classical' privacy would rely upon uncovering some piece of information which – due to some facet of privacy such as intimacy, seclusion, or dignity – an individual wanted to remain private. Or, a clear, direct and linear interference with our 'private sphere,' the character of which would vary given the context and particular circumstances.

However, modern data collection presents a threat of a different nature, allowing certain entities – whether private or public – to collate a sophisticated database of personal data the vast majority of which you would not consider to be private information; and would thus be content with entering the public realm. A collection of facts which you have exercised the normative choice to disclose, as the circulation of them does not impede upon – for example – your dignity, intimacy, or desire to be let alone. The entity in question processes this data, using sophisticated analysis to exercise control over you, or feeds them into automated systems which make potentially unfair decisions about you. This is an

intuitively recognisable harm, but not one which could be easily characterised as an invasion of privacy. In other words, the threat presented by the combination of big data and surveillance capitalism exists outside of considerations of privacy, and this is what separates data protection and privacy.[122]

Because the two rights respond to different threats, they function differently. De Hert and Gutwirth's 'opacity and transparently model' offers an insightful overview of this distinction.[123] This account posits that privacy performs an opacity function, as it has a prohibitive nature and shields individuals against interference. Data protection, on the other hand, seeks to ensure transparency as data protection rules acknowledge some form of data processing must take place, but controls the power of those who undertake the processing by 'devising legal means of control of these powers by the people.'[124] In other words, privacy (opacity) rules 'embody normative choices about the limits of power' while data protection (transparency) rules apply after this normative choice, to allow the processing of data, 'to channel the normatively accepted exercise of power.'[125]

This model provides a valuable conceptual distinction between the two rights, maintaining an understanding of privacy as a narrower, individual right while clearly portraying the role and character of the broader right to data protection. It also

[122] See also, Lee A. Bygrave, 'The place of privacy in data protection law' (2001) 7 University of New South Wales Law Journal forum 26, 28 'data protection laws serve a multiplicity of interests, which in some cases extend well beyond traditional conceptions of privacy'.

[123] Paul De Hert and Serge Gutwirth, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in Erik Claes, Antony Duff and Serge Gutwirth (eds), *Privacy and the criminal aw* (Intersentia 2006).

[124] Ibid 5.

[125] Ibid 70.

acknowledges the fundamental tension for which data protection law seeks to strike a balance, that some degree of personal information processing should be permitted, but we should regulate these practices in some way to protect individual rights. In other words, 'data protection is pragmatic; it assumes that private and public actors need to be able to use personal information because this is often necessary for societal reasons.'[126]

This raises the question: how does data protection function in such a way? To understand this further, we can refer to Lynskey's compelling account exploring the 'added-value' of the fundamental right to data protection outside of privacy, which advances two key claims.[127] Firstly, the right to data protection 'promot[es] informational self-determination and individual personality rights' by offering an extensive arsenal of informational rights which go above and beyond those conferred by the right to privacy.[128] Rights such as a general right to access, the right to be erasure and the right to data portability (which will be discussed at length later in this work) offer new tools for data subject control which privacy does not provide for. Furthermore, due to the broad definition of personal data, as all information on identified or identifiable persons, data protection rights apply to a much wider range of personal information compared to privacy, which is typically limited to information towards which one would have a reasonable expectation of privacy.

[126] Gutwirth and De Hert 3.

[127] Orla Lynskey, 'Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order' (2014) 63 International and Comparative Law Quarterly 569.

[128] Ibid 589.

This second key observation Lynskey makes is that data protection functions 'as a positive right to reduce information and power asymmetries.'[129] Power and information imbalances are created and exacerbated by information technologies and data protection seeks to prevent and correct these market failures by strengthening the position of the individual as concerning the data controller. In my view, this aspect of data protection law has great potential to confront and address the problems with modern big data analysis, but there is a lot of work to do to develop the law in this regard. This will be discussed at length throughout this work.

This account demonstrates both the value of data protection outside privacy, and the important role of informational self-determination in this respect. Data protection extends well beyond privacy, conferring extensive, easily accessible and widely exercised rights of control, going beyond those which privacy is capable of affording. In addition, it places limitations on the exercise of informational power which can reduce, prevent, and even subvert, these power asymmetries; potentially creating an environment where these rights of control can be exercised. These dual functions – which could be described as internal and external to informational self-determination – are absolutely vital, and of great importance to the assertions made throughout this work.

There is, admittedly, some degree of overlap between privacy and data protection, as exercising the right to privacy will at times involve exercising some degree of control over personal information, albeit not to the extent possible through data protection. In this sense, individual informational control does link the concepts together, but it is not the

[129] Ibid.

homogenising 'conceptual link' described by those who believe data protection is subsumed by privacy. A limited form of personal information control is one of the many facets of privacy. However, with regard to data protection, informational self-determination plays a key role.

European Data Protection Law

This thesis will proceed by analysing the jurisprudence of the ECtHR and the CJEU, focusing on how these courts view the relationship between privacy and data protection. Before doing so, however, it is necessary to establish the legislative provisions underpinning this case law, consisting of both human rights instruments and EU secondary legislation.

The European Convention on Human Rights (ECHR), in Article 8, proclaims that '[e]veryone has the fundamental right to respect for his private and family life, his home and his correspondence.'[130] There is no provision in the ECHR which specifically addresses the right to data protection. However, as will be discussed below, the ECtHR has extended and applied the right to privacy to cases involving issues of data protection. In 1970 the Council of Europe (CoE) responded to rising concerns over 'whether the right to privacy was capable of addressing the challenges posed by the technological developments

[130] European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, art 8.

of that time'[131] by adopting Convention 108,[132] 'the first ever binding international treaty addressing the need to protect personal data.'[133]

Compared to the approach taken by the CoE, the situation in the European Union (EU) is considerably more complex. The connection between EU law and the ECHR is identified in Article 6 of the Treaty on European Union (TEU),[134] which identifies the 'special role'[135] of the ECHR.[136] The EU Charter of Fundamental Rights (EU Charter) establishes the right to privacy in Article 7 which states, 'everyone has the right to respect for his or her private and family life, home and communications.'[137] This right directly corresponds to Article 8 ECHR, with the slight modification of replacing 'correspondence' with 'communications' to take into account developments in technology.

[131] Kranenborg 228.

[132] Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108; Convention 108 conferred legal obligations upon the relevant parties, member states of the Council of Europe, to enact necessary measures in relation to automated personal data files and automatic processing of personal data in the public and private sectors. These measures concerned quality of data (Article 5), special categories of data (Article 6), data security (Article 7), and additional safeguards for the data subject (Article 8). Convention 108 is widely acknowledged to have greatly influenced subsequent data protection regulation, including the DPD and the GDPR.

[133] 'Data Protection Day: 40 years of Convention 108' (*Council of Europe*, 27 January 2021) <https://www.coe.int/en/web/portal/-/data-protection-day-40-years-of-convention-108> accessed 14 April 2021.

[134] Consolidated version of the Treaty on European Union [2012] OJ C326/01, art 6.

[135] Marios Costa, Steve Peers and Josephine Steiner, *Steiner & Woods EU law* (14th edition edn, Oxford University Press 2020) 146.

[136] Despite being part of a separate legal system to EU law, it is acknowledged that there is a connection between the ECHR and The EU Charter, yet this relationship is somewhat unclear. For a more detailed discussion, see ibid 164-168.

[137] Charter of Fundamental Rights of the European Union [2007] OJ C303/01 (EU Charter), art 7.

Before 2009, the issue of data protection was predominantly addressed by the EU through secondary legislation. Notably, the Data Protection Directive was established on the 24th of October 1995.[138] The object of this legislation was to ensure that 'Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.'[139] With the adjoining objective of 'neither restrict[ing] or prohibit[ing] the free flow of personal data between Member States.'[140] Despite being repealed by the introduction of the General Data Protection Regulation (GDPR),[141] it is important to acknowledge this Directive for two reasons. Firstly, in many of the CJEU cases on data protection the court was asked to apply the provisions of the directive. Secondly, the directive included a number of provisions which afforded greater control to data subjects, albeit in a less extensive form than that afforded by the GDPR.[142] These include: the right to access one's data;[143] the right to object to processing in specific situations;[144] and the right not to be subject to a decision based solely on automated processing of data.[145]

[138] Directive 95/46/EC 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 [1995] OJ L 0031 (Data Protection Directive).

[139] Ibid art 1(1).

[140] Ibid art 1(2).

[141] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119 (GDPR).

[142] Shulga-Morskaya refers to this as the 'self-determination 'starter package' of rights', Shulga Morskaya (n 8) 6.

[143] Data Protection Directive, art 12.

[144] Ibid art 14.

[145] Ibid art 15.

In 2009, the EU recognised the right to protection of personal data as a fundamental right, through Article 8 of The Charter, 'everyone has the right to the protection of personal data concerning him or her.'[146] This coincided with the entry into force of the Treaty of Lisbon, which gave full legal effect to the provisions of the Charter[147] and elevated them to the same level as the treaties.[148] Paragraphs 2 and 3 of Article 8 of the Charter 'lay down some specific guarantees'[149] for the right to data protection. Declaring that '[s]uch data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.'[150] Furthermore, 'compliance with these rules shall be subject to control by an independent authority.'[151]

This was a landmark development in data protection and human rights law, as 'The Charter is unique in recognising the right to data protection.'[152] The inclusion of this fundamental right differentiates the Charter from other human rights instruments and was undoubtedly a strong declaration of intent from the EU concerning the protection of the fundamental rights of data subjects. Analysing this instrument, Kranenborg demonstrates that some parts align with informational self-determination, such as consent as a lawful

[146] EU Charter, art 8.

[147] Steve Peers and others (eds), *The EU Charter of Fundamental Rights : a commentary* (Hart Publishing 2014) vi.

[148] TEU, art 6(1).

[149] Juliane Kokott and Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222, 223.

[150] EU Charter, art 8(2).

[151] Ibid art 8(3)

[152] Kranenborg (n 115) 228.

basis for processing and mentioning initial control rights of access and rectification. However, the provision also 'looks beyond this,' recognising that there are other grounds for the processing of personal data, creating a system of checks and balances, and requiring oversight by an independent authority.[153] In other words, the Charter lays the foundation for data subject control, but also a system which regulates the power asserted by those who process personal data. This acts both internally and externally to informational self-determination and reflects Lynskey's account of the 'added-value' of data protection.

However, while the relationship between Article 7 of the Charter and Article 8 of the ECHR is clear and direct, the relationship between Article 8 of the Charter and the right to privacy in the ECHR is more complex.[154] The explanations state that Article 8 of the Charter is *based on* Article 8 ECHR but is also based on a number of other provisions; in particular – Article 286 of the EC Treaty (now replaced by Article 16 TFEU and Article 39 TEU), the Data Protection Directive, and Convention 108. Referencing a number of provisions concerning both privacy and data protection in this way creates ambiguity regarding the precise content of this right. As a result, the purpose of the fundamental right to data protection, and its relationship with the well-established right to privacy, was uncertain.

[153] Ibid 229.

[154] Ibid

With the relevant legislation established, this discussion will proceed with a doctrinal analysis of the case law of the ECtHR and the CJEU, observing how the courts interpret the relationship between the rights to privacy and data protection.

**The European Court of Human Rights: The Expansion of Privacy**

Despite the absence of any separate provision on data protection in the ECHR, the Strasbourg court has shown a great willingness to expand the notion of 'private life' to address data protection issues through Article 8.

This is shown through the development of 'private life' beyond the classical understanding of a 'private sphere.' In *Niemietz v Germany,* the court observed that private life is not restricted to an 'inner circle' and, in doing so, held that there is no reason to exclude 'activities of a professional or business nature' from this sphere.[155] In *Amann v Switzerland* the court held that merely 'the storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8.'[156] Furthermore, the ruling in *Pretty v The United Kingdom*[157] contains 'a very relevant and broad recognition of the principle of personal autonomy'[158] within privacy. The ruling describes private life as 'a broad term not susceptible to exhaustive definition,'

[155] *Niemietz v Germany* (1992) Series A no 251-B, para 29; see also Kranenborg (n 115) 235.

[156] *Amann v Switzerland* ECHR 2000-II 245, para 69.

[157] *Pretty v The United Kingdom* ECHR 2002-III 155, para 61; the case concerned whether the right to die with assistance could be recognised under the right to privacy, a claim which was not recognised.

[158] Gutwirth and De Hert (n 116) 15.

covering 'the physical and psychological integrity of a person… a right to personal development, and the right to establish and develop relationships.'[159]

This observation of the broad scope afforded to privacy by the ECtHR is well founded. In addition, other scholars have commented on the 'strong tendency'[160] to assert data protection rights within the scope of privacy, or that the jurisprudence 'gives rise'[161] to a right to data protection. De Hert and Gutwirth's systematic analysis of a wide range of case law demonstrates that the ECtHR has recognised a significant number of personal information 'control' rights commonly considered part of data protection law.[162] These include a right of access to personal files[163] and a right to erasure of personal data from public files.[164] The court has also acknowledged the fundamental data protection law principle of purpose limitation.[165] Furthermore, in a number of cases the court has emphasised the necessity of an independent supervisory authority to enforce these rights, similar to the requirement set out in Article 8(3) of the EU Charter.[166]

---

[159] *Pretty v The United Kingdom, para 61*; For further examples of the court expansive interpretation of 'private life' see *Rotaru v Romania* ECHR 2000-V 109, paras 33-34; *M.M. v The United Kingdom* App no 24029/07 (ECtHR, 13 November 2012), para 188.

[160] N. N. Purtova, *Property rights in personal data: A European perspective* (Corien Prins and others eds, Uitgeverij BOXPress, Oisterwijk 2011) 216.

[161] Kokott and Sobotta (n 149) 223.

[162] Gutwirth and De Hert 15-20.

[163] *Gaskin v the United Kingdom* (1989) Series A no 160; *Antony and Margaret McMichael v United Kingdom* (1995) Series A no 307-B; *Guerra v Italy* ECHR 1998-I; *McGinley & Egan v the United Kingdom* ECHR 2000-I.

[164] *Leander v Sweden* (1987) Series A no 116; *Segerstedt-Wiberg and Others v Sweden* ECHR 2006-VII 87.

[165] *Peck v the United Kingdom* ECHR 2003-I, para 62; *Perry v the United Kingdom* ECHR 2003-IX, para 40; *P.G. and J.H. v the United Kingdom* ECHR 2001-IX, para 59.

[166] *Klass v Germany* (1978) Series A no 28, para 55;*Leander v Sweden, paras 65-67*; *Rotaru v Romania, paras 59-60.*

An interesting development in this regard stems from the recent ruling in *Satamedia.*[167] In this case, the court explicitly states that Article 8 confers a form of the right to informational self-determination. After acknowledging the fundamental importance of personal data to the right to privacy in Article 8, and the obligations placed upon domestic legal systems to implement appropriate safeguards to protect personal data, the judgment states:

> Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged.[168]

Overall, the Strasbourg court has adopted a wide-ranging interpretation of the right to privacy through: an expansive definition of private life; the recognition of data protection rights; and even adopting the language of informational self-determination. In doing so, the court has subsumed data protection within privacy.[169] This may be viewed by some as a positive development, however, 'the very basis of data protection in Strasbourg is not as solid as it looks.'[170] Despite the broad understanding of 'private life in the ECtHR jurisprudence, it 'does not necessarily include all information on identified or identifiable persons.'[171] Data Protection law, on the other hand, covers precisely this and is not 'context

[167] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* (ECtHR, 27 June 2017) App no 931/13.

[168] Ibid, para 137.

[169] As observed by Gutwirth, the ECtHR has taken an expansive approach to privacy in a number of ways, including regarding environmental issues and excessive noise levels, see Gutwirth (n 106) 4.

[170] Gutwirth and De Hert (n 116) 24.

[171] Kokott and Sobotta (n 149) 225.

dependent.'[172] Additionally, the information rights conferred upon data subjects through data protection law are more extensive than those recognised by privacy. In *Leander*[173], the ECtHR 'stipulated rather bluntly'[174] that Article 8 ECHR does not afford 'a *general* right of access to personal data,'[175] a right which is explicitly recognised in data protection legislation. In addition to this, there are other data subject rights which are not recognised by the right to privacy in the ECHR, such as the right not to be subject to an automated decision, the right to erasure, and the right to data portability.[176] Furthermore, the conflation of the two rights creates confusion, thereby restricting the effectiveness and potential of data protection as a fundamental right. This discussion will now turn to focus on the case law of the CJEU, which has a separate and distinct fundamental right to data protection at its disposal.

**The Court of Justice of the European Union: Valuable Progress**

Before engaging in a critical analysis of the Luxembourg case law, it is necessary to acknowledge the progress made by the CJEU regarding the fundamental right to the protection of personal data. As previously stated, data protection has great potential to enhance the position of data subjects by affording them greater control over their personal information, and confront the information and power asymmetries caused by sophisticated data collection. We must recognise that the CJEU has, through a number of judgments , made notable progress in this regard in a range of ways. The analysis in this section will

[172] Lynskey (n 127) 583.

[173] *Leander v Sweden*

[174] Gutwirth and De Hert (n 116) 24.

[175] Ibid; emphasis added.

[176] Lynskey (n 127) 586.

focus on the following aspects: the strict definition of consent; the priority of fundamental rights over economic interests; and combating blanket surveillance and mass data retention.

*Definition of 'Consent':*

In data protection, the consent of the data subject is one of the main justifications for the lawful processing of data. The Data Protection Directive required 'unambiguous consent'[177] to be given by the data subject. This has been updated by the GDPR[178], by providing an extensive definition of consent in Article 4[179] and further details for the requirements of consent in Article 7.[180] In *Fashion ID GmbH v Verbraucherzentrale* (the Fashion ID case)[181] the court dealt with the issue of an online clothing retailer embedding the Facebook like button on their website. Upon visiting the website, due to the presence of the like button, the user's data was automatically transmitted to Facebook Ireland. In its ruling, the CJEU found the website operator to be a 'controller' and placed obligations upon them to inform the user of the processing, and to obtain the consent; regarding the transfer of data to Facebook.[182] Furthermore, in *Bundesverband der Verbraucherzentralen* (the Planet49 Case),[183] the court found that the user's consent to the use of cookies was not valid as, in order to refuse consent, the user was required to 'un-tick' a box which had been 'pre-ticked' by the service provider. The lack of affirmative consent did not meet the

[177] Data Protection Directive, art 7(a).

[178] GDPR, art 6(1)(a).

[179] Ibid, art 4(11).

[180] Ibid, art 7.

[181] Case C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* EU:C:2019:629.

[182] Ibid, para 106.

[183] Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* EU:C:2019:801.

strict requirements of the GDPR, as the court interpreted these provisions strictly.[184] As will be discussed at a later point in this thesis, there are overriding problems with the way consent functions in the context of extensive modern data collection practices. However, at this point it is worthwhile to consider that the CJEU's strict approach to the definition of consent is admirable, as it strengthens the position of the data subject, enhancing their ability to exercise informational self-determination.

*Fundamental Rights vs Economic Interests:*

Furthermore, the Luxembourg judges have shown a distinct willingness to prioritise the fundamental rights of the data subject, over the economic interests of data controllers. This is clearly exemplified in the landmark case *Google Spain SL v AEPD,*[185] where the CJEU, applying the provisions of the Data Protection Directive, recognised Mario Costeja González's 'right to be forgotten.' In doing so, the court required that Google Spain remove links on their search engine to website detailing a forced sale of Mr González's property due to his financial difficulties at the time.

The judgment explains that the processing of personal data carried out by a search engine 'is liable to affect significantly the fundamental rights to privacy and to the protection of personal data.'[186] This is of particular concern where the information can be accessed by searching the subject's name, especially so in the context of the heightened importance of the internet in modern society. The judgment continues, 'in the light of the

[184] For a similar ruling, see: Case C-61/19 *Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)* EU:C:2020:901.

[185] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* EU:C:2014:317.

[186] Ibid, para 80.

potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing.'[187]

The court goes on to state that where the exercise of these fundamental rights could have an effect on the legitimate interests of internet users in accessing this information, a fair balance should be sought.[188] However, the court is explicitly clear that when an individual seeks to exercise their fundamental rights, they will prevail over the economic interests of data controllers. This landmark ruling became the focus of widespread discussion and debate across the world, and is undoubtedly an invaluable development in the area of data protection law; recognising the data subject's informational self-determination and significantly strengthening their position with respect to data controllers who process data for economic gain.

*Combatting mass surveillance:*

Finally, in a series of judgments, the CJEU has used its powers to curtail mass surveillance and blanket data retention. The most notable judgment in this regard is *Digital Rights Ireland Ltd,*[189] in which the court was asked to provide a preliminary ruling on the validity of Directive 2006/24/EC of 15 March 2006 (The Data Retention Directive). The Directive in question required providers of publicly available electronic communications services or of public communications networks,[190] to retain certain data for an extended period of time,

[187] Ibid, para 81.

[188] Ibid, para 99.

[189] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd and Others v Minister for Communications, Marine and Natural Resources and others (Irish Human Rights Commission intervening)* EU:C:2014:238.

[190] Ibid, para 26.

for the purpose of possible access to them by competent national authorities in order to fight crime.[191] This data, as the court commented, 'may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained.'[192] The CJEU found the Data Retention Directive to be invalid as it 'derogates from the system of protection of the right to privacy'[193] established in the data protection legislation and constitutes a 'wide ranging [and]… particularly serious'[194] interference with Articles 7 and 8 of the Charter. The Commission had made an error in its proportionality analysis, under Article 52(1), regarding a justification for a limitation of those fundamental rights.[195] Such a derogation would only be justified if limited to what is 'strictly necessary'[196] for the purposes of combatting serious crime and, in the case at hand, 'sufficient safeguards'[197] were not in place to ensure this.

Subsequently, the preliminary ruling in *Joined Cases Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Watson*,[198] the CJEU upheld its decision in *Digital Rights Ireland*. It was held that national legislation providing for the general and indiscriminate retention of all traffic and location data for the purposes

[191] Ibid, para 29.

[192] Ibid, para 27.

[193] Ibid, para 32.

[194] Ibid, para 37.

[195] EU Charter, art 52(1).

[196] *Digital Rights Ireland Ltd, para 65*.

[197] Ibid, para 66.

[198] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* EU:C:2016:970.

of fighting crime was also invalid. The access to the retained data by competent public authorities was not permissible, as it was 'not restricted solely to fighting serious crime.'[199]

Furthermore, in *Schrems*, Austrian law student Maximillian Schrems filed a complaint regarding the transfer of his personal data from Facebook Ireland to servers in the US. [200] The complaint was originally rejected by the Irish Data Protection Authority as the transfer was approved under the 'Safe Harbour Scheme,' legally validated by EU Commission decision 2000/250, which determined that the US ensured an adequate level of protection of the data concerned. The CJEU found decision 2000/250 invalid, as the US did not provide for sufficient safeguards of the personal data, as US undertakings were able to disregard the protective rules, without limitation, for the purposes of national security and law enforcement. In the subsequent case *Schrems II*, the CJEU invalidated another agreement approved by the EU Commission to facilitate EU-US personal data transfers; the 'Privacy Shield Agreement.'[201] In doing so, the court also cited the lack of sufficient safeguards for the protection of personal data.[202] Therefore, in the context of international data transfers and state data collection, the court has demonstrated its ability to restrict blanket retention of personal data and implement strict safeguards, as such practices offer a significant threat to the fundamental rights of data subjects. [203]

---

[199] Ibid, para 125.

[200] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015:650.

[201] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Schrems II)* ECLI:EU:C:2020:559, para 201.

[202] Ibid, para 185.

[203] For other examples of mass surveillance cases, see: *Opinion 1/15 of the Court on the Draft Canada-EU data transfer agreement* EU:C:2017:592; Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* ECLI:EU:C:2020:790; Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others* EU:C:2020:791; Case C-708/18 *TK v Asociaţia de Proprietari bloc M5A-ScaraA* EU:C:2019:1064.

Overall, with regards to the CJEU jurisprudence, the judges 'did not hesitate' and adopted a 'bold and innovative'[204] approach in exercising their powers under the EU Charter. Through a variety of means – consent, protection of fundamental rights against economic interests, and combatting mass surveillance – the court made rulings which strengthened the position of the data subject and sought to address the power asymmetries resulting from advanced data collection.[205]

**The Court of Justice of the European Union: The Conflation of Privacy and Data Protection**

However, through a closer examination of the relevant case law, a particular concern arises regarding the judgments offered by the CJEU. That is, the ambiguous relationship between the fundamental rights of privacy and data protection.

Before the Treaty of Lisbon, and alongside it the recognition of data protection as a fundamental right in the Charter, the CJEU treated data protection as if it was contained within privacy. The court relied upon Article 8 ECHR and interpreted secondary data protection legislation in light of the convention. In the cases *Rundfunk*[206] and *Lindqvist*[207]

[204] Yves Poullet, 'Is the general data protection regulation the solution?' (2018) 34 The computer law and security report 773, (referring to the interpretation of the 1995 directive specifically).

[205] There are other positive developments of the CJEU jurisprudence in this regard which, due to the limitations of this thesis, it is not possible to discuss fully here. This includes the wide interpretation of 'data controller' in *Google Spain CL v AEPD, paras 35-38*; see also the recognition of 'joint-controllers' in *FashionID*; Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* EU:C:2018:388. Another notable development is the extensive powers afforded to national Data Protection Authorities, observed in *Schrems*; *Wirtschaftsakademie Schleswig-Holstein, para 62*

[206] Joined cases C-465/00, C-138/01 and C-139/01 *Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk* ECLI:EU:C:2003:294.

[207] Case C-101/01 *Criminal proceedings against Bodil Lindqvist* ECLI:EU:C:2003:596.

the court asserted the applicability of the Data Protection Directive with an 'absolute focus on privacy.'[208] In particular, in *Rundfunk* the court held that because there was a breach of Article 8 ECHR, the Data Protection Directive was also not satisfied. In doing so, the court did not comment on what would happen if it was found that Article 8 was not breached. Therefore, the judges 'entirely overlooked the specific rules set out in the Data Protection Directive'[209] and offered a conception of 'data protection as privacy, no more no less.'[210] Furthermore, in *Promusicae*[211] the court 'referred to privacy and data protection as one right'[212] and in *Satamedia*[213] 'the directive was treated as a privacy protection tool.'[214]

Following the entry into force of the Lisbon treaty, on the 1st of December 2009, the EU boasted a legally binding Charter of Fundamental rights with two distinct rights recognising the right to respect for private and family life, and to the protection of personal data. One might expect this to lead to a wealth of jurisprudence from the Luxembourg court detailing the nature of this new and unique right in Article 8, and clarifying its relationship with the right which precedes it. However, and unfortunately, in the post-Lisbon case law the court 'has consistently conflated the two rights.'[215]

---

[208] Gutwirth and De Hert (n 116) 32.

[209] Lynskey (n 127) 575.

[210] Gutwirth and De Hert (n 116) 33.

[211] Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* ECLI:EU:C:2008:54.

[212] Lynskey (n 127) 576.

[213] Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* ECLI:EU:C:2008:727.

[214] Lynskey (n 127) 576.

[215] Ibid 569.

In *Volker,*[216] one of the first data protection cases in this new regulatory context, Adovcate General Sharptson offered an acknowledgement of the difference between the two rights. Delivering her opinion, she described separate rights as 'a classic right (the protection of privacy under Article 8 ECHR) and a more modern right (the data protection provisions of Convention No 108).'[217] However, neither the AG's opinion nor the subsequent judgment offer any clarification or elaboration upon this relationship between the two rights or the substance of this 'more modern right'.[218] Moreover, in its judgment, the court consistently refers to the two articles in the charter 'in the same breath,'[219] with statements referring to the 'right to respect for private life with regard to the processing of personal data'[220].

Analysis of the subsequent CJEU cases demonstrates the continuation of the 'fundamental rights hybrid'[221] observed in *Volker*. In *Digital Rights Ireland*, the AG does state that Article 8 of the Charter is 'distinct from the right to privacy,'[222] but only refers to the existence of secondary data protection legislation to show this. Furthermore, they state that 'data protection seeks to ensure privacy,'[223] and directly references the combination

[216] Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* ECLI:EU:C:2010:662.

[217] Ibid, Opinion of AG Sharpston, para 71.

[218] Lynskey (n 127) 579.

[219] Kranenborg (n 115) 230.

[220] *Volker und Markus Schecke and Eifert,* para 52.

[221] Paula Filipová, 'The impact of the CJEU case law on the interpretation of the fundamental rights to privacy and data protection' (Master's Thesis, Charles University 2017) 57.

[222] *Digital Rights Ireland Ltd Opinion of AG P Cruz Villalón, para 55*.

[223] Ibid, Opinion of AG P Cruz Villalón, para 55.

put forward in *Volker,* as the rights are 'so closely linked.'[224] The judgment follows a similar merged understanding of the two rights, referring to the 'the important role played by the protection of personal data in the light of the fundamental right to respect for private life.'[225] As a result, the 'relationship between Article 7 and 8 of the Charter remains in the dark.'[226] The blurred distinction continues in *Google Spain*, in which Advocate General Jääskinen identified 'the wide interpretation given by the court to the fundamental right to private life in a data protection context.'[227] Outlining the rights in this manner, implying that the broad scope of the right to privacy encompasses data protection, is very similar to the reasoning of the ECtHR.

Through close consultation of the CJEU jurisprudence, a consistent trend emerges. While rulings are substantial, and attract attention as symbolic achievements for data protection, the case law 'does not reveal a clear approach'[228] regarding the relationship between the fundamental rights of privacy and data protection. Offering an explanation, De Hert and Gutwirth deploy Lessig's observation of 'transformative,' as opposed to codifying, constitutions. According to Lessig, in addition to codifying constitutions which codify fundamental values in a legal order, there are also 'transformative' constitutions with a more progressive purpose, seeking to develop or change the essential and well-established values.[229] As data protection is a relatively new concept, its recognition as a

[224] Ibid, Opinion of AG P Cruz Villalón, para 62.

[225] Ibid, para 48.

[226] Filipová (n 221) 64.

[227] *Google Spain CL v AEPD, Opinion of AG Jääskinen, para 29*.

[228] Kranenborg (n 115) 229.

[229] Lawrence Lessig, *Code : and other laws of cyberspace* (Basic Books 1999).

fundamental right in the EU Charter has a certain transformative effect. When lawmakers seek to develop values in this way, it is often the case that 'the courts do not feel certain about them, [and] they might resort to more familiar old values.'[230]

This lack of clarity raises issues regarding the status of Article 8, and the role it plays as an 'overarching fundamental right.'[231] As observed by a number of scholars, 'Data protection does a lot more than echoing a privacy right with regard to personal data,'[232] this distinction has 'deeper character'[233] and 'the specifics of each right must be respected.'[234] Any suggestion otherwise represents an unfortunate interpretation of the relevant concepts and limits the effectiveness of data protection as a fundamental right.

Summary

This chapter began by asserting the crucial significance of the right to informational self-determination in response to the problems explored in chapter one. It then proceeded to outline the importance of data protection as a distinct right separate from privacy, building upon the 'opacity and transparency' model but focusing more specifically on Lynskey's account of the added-value of data protection. In this regard, the importance of data protection is demonstrated by its dual functions; both internal and external to informational

[230] Gutwirth and De Hert (n 116) 12-13.

[231] Kranenborg (n 115) 240.

[232] Gutwirth and De Hert (n 116) 5.

[233] Ibid 10.

[234] Kokott and Sobotta (n 149) 222.

self-determination. In order to solve the problems created by the data economy, both of these aspects of data protection must be fully developed.

However, despite these claims, data protection remains a somewhat infantile and under-developed right, yet to realise its potential. This can be demonstrated by an analysis of the ECtHR and CJEU jurisprudence which demonstrates that, despite valuable progress, both courts merge the two rights together and treat them as interchangeable. Continuing the analysis of data protection law, the following chapter will focus on the landmark EU legislation – the GDPR.

# Chapter Three – The General Data Protection Regulation

*'Nothing appears more surprising to those, who consider human affairs with a philosophical eye, than the easiness with which the many are governed by the few; and the implicit submission, with which men resign their own sentiments and passions to those of their rulers.'*

- David Hume, *Of the first principles of government,* 1741[235]

## Introduction

As discussed in the previous chapter, the right to data protection can offer great value to address the emerging problems of the data economy. Although, the lack of clarity regarding the unique status of this right, particularly in judicial reasoning, limits such potential. The introduction of the GDPR, however, appears to represent much-needed development in this area of law. The regulation presents itself as a data protection statute, as demonstrated by the title and its foundational sections. Where the 1995 Directive was concerned with the right to privacy,[236] Article 1 of the GDPR cites only the right to the protection of personal data[237] with, thankfully, no use of the privacy-data protection hybrid adopted by the judges of the CJEU. It is an incredibly high-profile legal instrument, widely cited as the 'gold-standard' of data protection law.

The purpose of this chapter is to closely analyse the GDPR, in particular the provisions which seek to confer informational self-determination upon data subjects. The

[235] David Hume, 'Of the first principles of government' in Knud Haakonssen (ed), *Hume: Political Essays* (Cambridge University Press 1994) 16.

[236] Data Protection Directive, art 1(1)

[237] GDPR, art 1(1).

valuable progress made by the legislation will be outlined, before a comprehensive discussion of consent as a basis for lawful processing of data, and the wide range of data subject rights upheld by the regulation. Before doing so, however, this work will briefly elaborate upon the specific methodological approach to this discussion.

The Law on the Books and the Law in Action: A Note on Methodology

The introduction to this thesis offered an outline of the methodological approaches taken in each chapter. While I do not intend to become caught up in lengthy discussions of methodology, further elaboration of the type of perspective offered in this chapter will be useful. The approach taken is what Khatian and Steel refer to as an empirical theoretical method.[238] As opposed to an ontological theory (which seeks to understand the nature of a phenomenon) or a normative theory (concerned with the norms and values which justify an area of law), empirical theories are primarily concerned with the causal features and effects of law.'[239] They seek to explore the actual functioning of legal actors and institutions and identify any gaps between the 'law in action and the law on the books.'[240] Such inquiries have been very successful in the past at exposing how underlying power dynamics – or socioeconomic, political and cultural circumstances – shape and disrupt the proper functioning of the law. Khatian and Steel use the example of critical race theorists exposing the true motivations behind the landmark civil rights decision in *Brown v Board*

[238] Khaitan and Steel (n 5) 19.

[239] Ibid.

[240] Ibid 21; this phrase was first coined in Roscoe Pound, 'Law in Books and Law in Action' (1910) 44 American law review 12.

*of Education,*[241] and the subsequent barriers to racial integration in the United States.[242] Another example which comes to mind is the work of feminist legal scholarship on sexual offences. Demonstrating that, despite the valuable legislative development from a standard based on violence to one of consent, flaws in judicial procedure and the continued prevalence of misconceptions regarding rape and sexual offences throughout the general public, left systemic problems and victims continue to be unable to find justice as a result.[243]

While I have not conducted any original and lengthy statistical analysis, due to the limitations of this thesis, this chapter adopts an critical lens which aligns to an empirical normative theory. It seeks to closely analyse the GDPR in the context of big data and surveillance capitalism to demonstrate the underlying flaws in its provisions, referring to more strictly 'empirical' studies in the process. The overarching conclusion I seek to demonstrate is that, while the regulation is a significant legislative achievement, due to problematic and widespread data processing practices, in reality it does very little to improve the circumstances of data subjects. As a result, the GDPR becomes a symbolic achievement and focusing on the value of its provisions in principle encourages complacency. A well rounded discussion in this regard must begin with an acknowledgment of the regulation's achievements, which is the focus of the following section.

---

[241] Khaitan and Steel 21; referring to *Brown v Board of Education* 347 US 483 (1954).

[242] See Mary L. Dudziak, 'Brown as a Cold War Case' (2004) 91 The Journal of American History 32; Derrick A. Bell, Jr., 'Brown v. Board of Education and the Interest-Convergence Dilemma' (1980) 93 Harvard Law Review 518.

[243] See: Sharon Cowan, 'Sense and Sensibilities: A Feminist Critique of Legal Interventions against Sexual Violence' (2019) 23 Edinburgh Law Review 22; Sandra Walklate, 'What is to be Done About Violence Against Women?' (2008) 48 The British Journal of Criminology 39.

The Progress of the GDPR: Declarations, Harmonisation and Individual Rights

The General Data Protection Regulation came into force on the 25th May 2018, repealing and replacing the 1995 Data Protection Directive. The EU Commission chose to introduce a regulation, as opposed to a directive, for the purpose of harmonising the rules concerning personal data protection across the EU member states.[244] Another fundamental purpose was to modernise, update and improve the legal framework in response to advancements in technology and data processing practices.

Article 1 sets out the subject matter and objectives of the legislation, which 'lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.'[245] Subsections 2 and 3 develop upon this to outline the two fundamental objectives: the regulation 'protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data'[246] while also providing for 'the free movement of personal data within the union.'[247] In doing so, the legislation sets out the tension at the heart of data protection law, that there are great opportunities and valuable benefits to be gained from the processing of personal data, but these practices present significant risks to civil liberties, and a well-functioning data economy cannot come at the expense of individual rights.

[244] GDPR, recital 3.

[245] Ibid, art 1(1).

[246] Ibid, art 1(2).

[247] Ibid, art 1(3).

In the remainder of the regulation, a wide definition of 'personal data' is outlined in Article 4, as 'any information relating to an identified or identifiable natural person.'[248] Article 5 establishes the key principles relating to processing of personal data, the first of which is that it must be 'processed lawfully, fairly and in a transparent manner.'[249] The remaining principles are 'purpose limitation,' 'data minimisation,' 'accuracy,' 'storage limitation,' 'integrity and confidentiality,' and 'accountability.'[250] In accordance with Article 6, processing of personal data is lawful if such processing is: approved on the basis of the data subject's consent; necessary for the performance of a contract to which the data subject is party; necessary for compliance with a legal obligation on the part of the controller; necessary to protect the vital interests of the data subject; necessary for a task carried out in the public interest; or necessary for the purposes of the legitimate interest pursued by the controller.[251] Furthermore, the GDPR places strict obligations upon data controllers to comply with the provisions,[252] affords more extensive powers to Independent Supervisory Authorities,[253] and creates new remedies available to data subjects to exercise their rights.[254]

The concept of informational self-determination appears central to the objectives of the GDPR. Recital 7 explicitly states that 'the framework is based on control and

[248] Ibid, art 4(1).

[249] Ibid, art 5(1)(a).

[250] Ibid, art 5(1)(b-f), (2).

[251] Ibid, art 6(1)(a-f).

[252] Ibid, arts 24-43.

[253] Ibid, arts 51-59.

[254] Ibid, arts 77-84.

certainty' and that 'natural persons should have control over their personal data.'[255] It has been observed that informational self-determination makes two claims: the importance of consent as a ground for processing; and that individuals should have various rights to exercise.[256] In this regard, the regulation upholds a strict standard for consent as a lawful basis for personal data processing and confers an extensive list of rights upon individual data subjects; providing them with the means to exercise control over their personal data. As Shulga-Morskaya states, 'such a range of rights composing the emerging right to informational self-determination raises the question of how these rights can be exercised in practice.'[257] This question, the functioning, strength and exercisability of informational self-determination, through the GDPR, in the context of the data economy is the focus of this chapter. This account will explore this question by analysing these two facets of informational self-determination; consent and data subject rights.

## The GDPR in Action: The Unfeasibility of Informational Self-Determination?

### Consent

Consent has an impactful and intuitively recognisable 'normative force' in everyday interpersonal relations in modern society, where we respect individuals as autonomous moral agents.[258] The doctrine confers upon us a 'certain agential ability' to bring about normative changes in the world. For example, by rendering permissible a certain previously

[255] Ibid, recital 7.

[256] Bert-Jaap Koops, 'The trouble with European data protection law' (2014) 4 International Data Privacy Law 250, 251.

[257] Shulga Morskaya (n 8) 7.

[258] For an account which explores the various ways through which consent exhibits this 'normative force', see Heidi M. Hurd, 'The Normative Force of Consent' in Andreas Müller and Peter Schaber (eds), *The Routledge handbook of the ethics of consent* (Routledge 2018) .

impermissible action.[259] Consent also plays an integral role in the concept of informational self-determination, as the principal means through which individuals can exercise control over their personal information. In this respect, 'consent requests fulfil a practical purpose, as they allow individuals to express their preference… [or] function as a warning that there may be consequences of a particular choice.'[260]

As previously stated, the lawmakers who constructed the GDPR seem to promote the right to informational self-determination by affording a central role to consent within the regulation. Detailing the provisions more extensively, consent is the first optional basis for the lawful processing of personal data, requiring that 'the data subject has given consent to the processing of his or her personal data for one or more specific purposes.'[261] Further provisions establish strict requirements for this consent, which must be 'freely given, specific, informed and unambiguous' and offered through 'a clear affirmative action.'[262] Article 7 sets out further conditions for consent, stipulating that the controller is under a duty to demonstrate that consent has been given,[263] it must be in a clearly distinguishable manner,[264] and that the data subject has the right to withdraw consent at any time.[265]

[259] For an account which seeks to explain the underlying nature and justification of this normative power, see Felix Koch, 'Consent as a Normative Power' in Andreas Müller and Peter Schaber (eds), *The Routledge handbook of the ethics of consent* (Routledge 2018).

[260] Bart Custers and others, 'Consent and Privacy' in Andreas Müller and Peter Schaber (eds), *The Routledge handbook of the ethics of consent* (Routledge 2018) 247.

[261] GDPR, art 6(1)(a).

[262] Ibid, art 4(1).

[263] Ibid, art 7(1).

[264] Ibid, art 7(2).

[265] Ibid, art 7(3).

Unfortunately, despite the important role of consent in the regulation – and the strict wording of the articles – it is widely accepted that data subjects do not engage with consent requests in the kind of meaningful and considered way required to constitute true informational self-determination. This situation has been labelled the 'mythology of consent' and described as 'largely theoretical with no practical meaning.'[266] In a 2009 speech the Federal Trade Commission (FTC) Chairperson John Leibowitz stated, 'we all agree that consumers don't read privacy policies.'[267] In an account which extensively details the various issues which limit the proper functioning of consent, Custers et al. observe that 'people seem to become increasingly disengaged in the consent processes' and that such passive interaction with consent mechanisms undermine their important role in exercising individual autonomy.[268]

This state of affairs raises the question: why have we collectively become so detached from the primary means of exercising control over our data? I would assert – and I am by no means the first to make this claim – that this is because the exercise of valid consent is not possible in the environment in which we are expected to do so.

Beginning with the requirement that consent is 'freely given,' unambiguous,' and made through a 'clear affirmative action,' the GDPR has made some valuable progress concerning these standards of voluntariness and clear intention on the part of the data subject. The regulation clearly prohibits accepting silence, pre-ticked boxes or inactivity as

[266] Koops (n 256) 251.

[267] John Leibowitz, 'Introductory remarks at the FTC Roundtable' (*FTC*, 7 December 2009) <https://www.ftc.gov/public-statements/2009/12/introductory-remarks-ftc-privacy-roundtable> accessed 14 April 2021.

[268] Custers and others (n 260) 253.

constituting consent.[269] In addition, as discussed in Chapter Two, the CJEU has strictly enforced these requirements. However, the proliferation of the IoT poses a threat to this. As we become increasingly surrounded by these devices, which are constantly collecting information, our consent becomes significantly less clear or voluntary. In other words, these 'rendition practices… overwhelm any reasonable discussion of opt-in and opt-out.'[270]

Even if we are to maintain that consent in this context remains 'voluntary', could we realistically consider it to be 'informed' and 'specific'? With regards to the information provided to the data subject, the GDPR exhibits strict requirements. The data subject has the right to be informed even where consent is not the relevant basis for processing, this places transparency obligations upon data controllers to provide information in an easily visible, intelligible and clearly legible manner.[271] When collected on the basis of consent the information provided must include the controllers identity[272] and the purposes of processing.[273] However, even if the information is provided, the data subject is still required to read through lengthy and complex 'privacy policies.' A widely cited study by two Carnegie Mellon Professors in 2008 estimated that if an American Internet user were to read every single one of these policies they encounter, it would take 244 hours per year.[274] Given the increased use of – and reliance upon – the internet since 2008 it is not

[269] GDPR, recital 32.

[270] Zuboff (n 25) 240; For a discussion of the barriers to consent in the IoT environment, see Sandra Wachter, 'Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR' (2018) 34 Computer Law and Security Review, 445-448.

[271] GDPR, art 12(6); see also arts 13-14.

[272] Ibid, recital 42.

[273] Ibid, recital 43.

[274] Aleecia M. McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 A Journal of Law and Policy for the Information Society 543, 563.

unreasonable to suggest that such a process would be significantly lengthier today. Furthermore, the requirement of 'specific' is particularly doubtful, given the nature of big data processing, which requires that massive amounts of data are collected over a long period of time, to undergo complex analysis in order to glean insights and make conclusions.[275] As Mayer-Schönberger and Cukier observed, the true value of big data is in its re-use beyond the original purpose of collection,[276] how can data subjects provide specific consent to such processing?

Looking beyond the specific requirement of the legislation, another flaw in consent can be observed regarding decisional capacity.[277] This concept requires that the decisionmaker has the ability to understand the factors involved in the decision and the potential consequences. A great deal of focus is placed on capacity as an aspect of consent in areas such as medical law, particularly with regard to children and young adults acquiring the capacity to consent to medical treatment. In many situations, human beings possess the capacity to provide valid consent, and respecting this is an important part of treating them as an autonomous moral agent. In addition, there will be some forms of data processing where such capacity is present. However, there are certain aspects of big data analytics which are so intricate and complex that an individual's capacity to understand what they are allowing – and the potential consequences – can be brought into question.

[275] See Custers and others (n 260) 251.

[276] Mayer-Schönberger and Cukier (n 24) 104-107.

[277] Discussing the 'validity of consent', Bullock emphasises the importance of decisional capacity, alongside informed and voluntariness requirements, Emma C. Bullock, 'Valid Consent' in Andreas Müller and Peter Schaber (eds), *The Routledge handbook of the ethics of consent* (Routledge 2018), 86-87.

One of the most attractive qualities of Artificial Intelligence (AI), to anyone who seeks to use it, is that through machine learning these systems are uniquely capable of working through vast data sets and identifying patterns. Machines have proven to be far more effective at this than human brains.[278] Significant questions can be raised as to whether a data subject has sufficient decisional capacity to consent, and to allow data to be fed into these systems which are – by their very nature – beyond human comprehension. Furthermore, this problem is showing signs of getting worse, as the technologies involved are growing in sophistication at an exponential rate, and such a rate of progression is not something human beings are readily capable of understanding.[279] The advancements in data processing technologies have created systems which, at times, go beyond human beings' limited capacity to make rational decisions.[280]

Another important point to note is that the flaws in the functioning of consent extend into other provisions of the directive. While the regulation places heightened importance upon the processing of 'special categories'[281] of personal data – by prohibiting such practices – this rule does not apply where the data subject has given 'explicit consent'[282] or manifestly made such data public.[283] As Zarsky observes, it is questionable whether this 'explicit consent' requirement really offers anything substantial to separate

[278] See, for example, Ewen Callaway, '"It will change everything": DeepMind's AI makes gigantic leap in solving protein structures' (*nature*, 30 November 2020) <https://www.nature.com/articles/d41586-020-03348-4> accessed 01 February 2021.

[279] See Pedro Domingos, *The master algorithm : how the quest for the ultimate learning machine will remake our world* (Allen Lane 2015) 73.

[280] See Koops (n 256) 252.

[281] GDPR, art 9; these include data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and certain genetic and health data.

[282] Ibid, art 9(2)(a).

[283] Ibid, art 9(2)(e).

these types of data.[284] Furthermore, while data subjects have the right not to be subject to a decision – which produces legal effects concerning them – based solely on automated processing, including profiling,[285] the subject can waive this right through explicit consent.[286]

**The Rights of the Data Subject**

As previously stated, the GDPR confers upon data subjects a range of rights, which aim to facilitate the exercise of control over personal data. These rights sit alongside consent, representing the two main aspects of informational self-determination in the regulation. The previous discussion demonstrated that the practical functioning of consent is problematic, as the burden to exercise this ability is placed upon individuals, within a context where it is inherently difficult to do so. This also encapsulates the problem with exercising data subject rights. While the law on the books appears to strengthen the position of individuals, an observation of the 'law in action' raises questions regarding the exercisability of these rights.

A number of the GDPR data subject rights had previously been part of the 1995 Directive, these include the right to be informed, to access[287], to rectify[288], to object,[289] and

[284] Zarsky (n 65) 1012.

[285] GDPR, art 22.

[286] Zarsky 1015.

[287] Data Protection Directive, art 15.

[288] Ibid, art 16.

[289] Ibid, art 21.

not to be subject to automated decision making.[290] Regarding these rights, minor but welcome changes were made to encourage and improve exercisability. For example, where before a data subject could be charged for making a request to access their data,[291] the GDPR only allows controllers to charge a reasonable fee for administrative costs where the data subject requests further copies.[292] In addition to these rights, the GDPR also substantially extended the right to erasure,[293] and introduced an entirely new right to data portability.[294] The following sections will analyse these two rights in more detail.

*The Right to Erasure (Right to be Forgotten)*

The Data Protection Directive contained a restricted right to erasure, within the subsections of the right to access. This was limited to 'processing which does not comply with the provisions of this Directive, in particular because of the complete or inaccurate nature of the data.'[295] The GDPR developed this right substantially by expanding the grounds under which the 'data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her.'[296] Most notably, to cases where the personal data are no longer necessary in relation to the purposes for which they were collected, where the

[290] Ibid, art 22; this right was modified by the GDPR, previously it would only apply to automated decision making intended to evaluate certain personal aspects relating to the data subject. Under the GDPR it now applies to such decisions which produce legal effects concerning the data subject, see GDPR art 22.

[291] The right to access in the Data Protection Directive only prevented 'excessive expense' on the part of the data subject.

[292] GDPR, art 15(3).

[293] Ibid, art 17; the regulation also introduced the right to the restriction of processing (Article 18), as a lesser alternative to the right to erasure.

[294] Ibid, art 20.

[295] Data Protection Directive, art 12.

[296] GDPR, art 17(1).

data subject withdraws consent, or where the data subject objects under Article 21.[297] This represents a valuable development for data subjects seeking to exercise control over their data, granting them 'an advantageous position and a huge authoritative boost'[298] and codifying the 'right to be forgotten' first recognised in *Google Spain.*[299]

Bearing in mind the dynamics and complexities of data processing activities, one is led to question whether the exercise of such a right – which appears strong and impactful – is a feasible endeavor. Some recent empirical studies have sought to answer this question, and uncovered some illuminating insights. One such study analysed changes to company 'privacy policies' following the enactment of the GDPR.[300] While the authors acknowledged progress had been made, they stressed that more progress is necessary and specifically identify the user's ability to delete information as an area where protection has worsened; observing an 'alarming level (57%) of non-compliance to the GDPR in new policies.'[301] Another study exemplifies this in more detail, by delving into the 'specific implementation challenges of the right to be forgotten.'[302] Through a review of the relevant literature, they identify some of the main barriers to implementation. These include the prevalence of 'data backups' and the 'development and increased usage of cloud services,'[303] which present difficulties in keeping track of data, identifying and erasing it.

[297] Ibid, art 17(1)(a-c).

[298] Vincenzo Mangini, Irina Tal and Arghir-Nicolae Moldovan, 'An empirical study on the impact of GDPR and right to be forgotten - organisations and users perspective' (Proceedings of the 15th International Conference on Availability, Reliability and Security).

[299] *Google Spain CL v AEPD*.

[300] Razieh Nokhbeh Zaeem and K. Suzanne Barber, 'The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise' (2020) 12 ACM Transactions on Management Information Systems 1
[301] Ibid, 18.

[302] Mangini, Tal and Moldovan (n 298) 1.

[303] Ibid 2; referring to Eugenia Politou and others, 'Backups and the right to be forgotten in the GDPR: An uneasy relationship' (2018) 34 The computer law and security report 1247; Andree E. Widjaja and others,

It must be acknowledged that the survey conducted by the researchers regarding public opinion towards the legislation – in particular the right to erasure – received positive responses overall; however 70% of respondents had not attempted to exercise the right.[304] Users approved of the legislation but indicated that they would like to see further improvements to the provisions, and that there still exists a 'general mistrust' in the companies who collect data.[305] This suggests that issues in implementation of the GDPR are not entirely attributed to complexities of data processing, there is also an overall power imbalance between data subjects and controllers leading to, amongst other things, a lack of trust in the data economy.

One report by the European Network and Information Security Agency offers a particularly damning assessment of the right to erasure.[306] Explaining that, in an open system such as the World Wide Web it is not possible for a person to locate all the data items stored about them, there are also difficulties in determining whether they have the right to request removal and the prospect of deleting all copies appears impossible. The report points to the underlying flaw that 'unauthorised copying of information by human observers is ultimately impossible to prevent by technical means.'[307] Furthermore, even in a closed system (such as a corporate network) erasing personal data is technically challenging and requires substantial operational overhead.

'Understanding users' willingness to put their personal information on the personal cloud-based storage applications: An empirical study' (2019) 91 Computers in human behavior 167.

[304] Mangini, Tal and Moldovan (n 298) 6.

[305] Ibid.

[306] Peter Druschel, Michael Backes and Rodica Tirtea, *The right to be forgotten - between expectations and practice* (European Network and Information Security, 2012).

[307] Ibid 8.

*The Right to Data Portability:*

In perhaps the most notable expansion of data subject rights, the GDPR introduced the right to data portability;[308] which allows a data subject to receive the personal data they have allowed to be processed (or have been processed by automated means) and have it transferred to another controller. The data subject also has the right to have the personal data transmitted directly from one controller to another, where technically feasible,[309] providing an alternative means to achieve this portability. This offers great potential to improve the circumstances of the data subject, and was described by the European Data Protection Supervisor (EDPS) in 2015 as 'the gateway in the digital environment to the user control which individuals are now realising they lack.'[310] However, a closer analysis of the provisions demonstrates distinct drawbacks and barriers to practical exercisability, similar to those regarding the right to erasure.

Firstly, concerns have been raised regarding the content of the right itself, as Article 20 states, the data subject has the right to data portability with respect to personal data 'which he or she *has provided* to a controller.'[311] This raises issues of scope, as a restrictive interpretation of 'provided' would exclude any information which has been received, observed, inferred or predicted by the data controller.[312] If the right to data portability does not apply to received or observed data, because these are not explicitly provided by the

[308] GDPR, art 20.

[309] Ibid, art 20(2).

[310] EDPS Opinion 3/2015 of 27 July 2015, Europe's big opportunity: EDPS recommendations on the EU's options for data protection reform; furthermore, Recital 68 of the GDPR clearly sets out the purpose of this new right 'to further strengthen the control over his or her own data'.

[311] GDPR, art 20(1) (emphasis added).

[312] Paul De Hert and others, 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services' (2018) 34 The computer law and security report 193, 199.

individual, it will not include data collected through cookies or location services. The omission of such data significantly restricts the declared purpose of data portability, to enhance user control. Furthermore, the right does not cover predictions or inferences drawn from the collection of personal data. Data subjects have the ability to move the personal data fed into systems – which process the data through automated means revealing insights regarding the individuals, including profiling – but they 'cannot control or move the inferences.'[313] As previously discussed, it is this sophisticated analysis and profiling which raises deep concerns regarding unfair treatment and the manipulation of vulnerable individuals. This is, therefore, a significant oversight of the regulation, which fails to address the complexities of the data processing or restrict the power of data controllers. Furthermore, Li observes an 'emerging but overlooked conflict'[314] between the right to data portability and the right to be forgotten. This account details the 'obvious' incompatibility between the two rights, as 'the unilateral exercise of the right to be forgotten by one data subject will deprive others of the chance for exercising the right to data portability.'[315]

Beyond the specific inadequacies regarding the provisions of the regulation, empirical studies have demonstrated the range of difficulties faced by data subjects in the context of data portability. Urquhart et al. point out that there are a number of emerging personal information management systems (PIMS), platforms which could potentially facilitate the exercisability of data portability. However, the writers detail an extensive

[313] Lachlan Urquhart, Neelima Sailaja and Derek McAuley, 'Realising the right to data portability for the domestic Internet of things' (2018) 22 Personal and Ubiquitous Computing 317, 326.

[314] Wenlong Li, 'A tale of two rights: exploring the potential conflict between right to data portability and right to be forgotten under the General Data Protection Regulation' (2018) 8 International Data Privacy Law 309, 317.

[315] Ibid 312.

range of 'technical barriers and implementation challenges.'[316] These include low usability, as data portability is a 'distant concept for the average user because of the highly technical nature of the subject' and hyberbolic discounting, as the user perceives the value of actions which ensure privacy to be lower that the rewards for using the service itself. Also, there is an issue of user trust management – data subjects want to place data with organisations they trust and there is a lack of well-known and trustworthy organisations who could act as bona-fide data stewards. The writers also observe more technical issues, such as data format inconsistencies, platform differences, and policy differences of platforms involved – which create barriers to an effective right of data portability.[317]

Other studies have further demonstrated these issues in practice, one example being a project by Turner and others which offers 'the first empirical investigation into the nascent IoT environment.'[318] The research conducted two separate studies, the first being a review of 160 'privacy policies,' which found that only 39% explicitly referenced data portability. Furthermore, the researchers found a prevalence of vague statements such as 'you have a right to data portability' with no further explanation. One particularly insightful observation was that none of the privacy policies outline how the data subject should actually go about approaching the controller to acquire their data. The other part of the study, which attempted to exercise the right to data portability with respect to four devices from prominent Big Tech companies, found that it was simply 'not possible to transmit data from one controller to another under Article 20.'[319] Amazon even treated the

[316] Urquhart, Sailaja and McAuley (n 313) 325.

[317] Ibid 325-326.

[318] Sarah Turner and others, 'The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment' New Media & Society <https://doi.org/10.1177/1461444820934033> accessed 28 March 2021, 2.

[319] Ibid 12.

researchers' request as a 'right of access' request under Article 15. Wong and Henderson conducted a similar study, making 230 data portability requests and observing a similar range of difficulties.[320] One particular issue they uncovered was – even though the GDPR requires that the data be communicated 'in a structured, commonly used and machine-readable format' there exists a 'lack of standards for managing the appropriateness of file formats' and widespread inconsistencies in the information they received.[321]

Underlying Cause: Complexities and Asymmetries of Power

The above discussion demonstrates an assortment of practical drawbacks to both the doctrine of consent and the exercisability of data subject rights in the GDPR. The provisions which seek to confer informational self-determination upon data subjects become burdensome, as opposed to their intended purpose of empowerment. As to the fundamental cause of these circumstances, this could be attributed to the complexities of big data analysis. A common critique of the GDPR is that it does not sufficiently take into account and counter the complexities of personal data processing practices.[322] As stated by Bygrave, 'it is questionable whether EU lawmakers, when drafting the GDPR, fully appreciated all of the regulatory challenges thrown up by machine learning and big data analysis.'[323]

---

[320] Janis Wong and Tristan Henderson, 'The right to data portability in practice: exploring the implications of the technologically neutral GDPR' (2019) 9 International Data Privacy Law 173.

[321] Ibid 185-186.

[322] Zarsky (n 65) offers a critique which claims the fundamental principles of the GDPR, such as 'purpose limitation' and 'data minimisation', are 'incompatible' with the complexities of big data analytics.

[323] Bygrave (n 9) 13.

However, a more fundamental and unsettling concern exists beyond a legislative failure to effectively respond to the complexities of personal data processing. The empirical accounts of data subjects' inability to exercise control are symptomatic of the drastically uneven power dynamic throughout the data economy. When attempting to exercising consent, for example, individuals are surrounded by devices which constantly collect their data, helplessly under-informed, and may even lack the capacity to fully understand the processes which impact upon them in order to make a valid decision. The doctrine of consent should, and does, carry great normative weight, and is 'useful [when] power is exerted in a small and ad hoc way,' however it is 'problematic for long-term power relationships with tech firms… [and] does not protect us at a systemic level from abuses.'[324] The provisions of the GDPR which provide the data subject with the ability to exercise control over their data are not sufficient when that individual is situated in a vulnerable position in relation to the powerful data controllers.[325] In other words, 'individuals each wrestling with the myriad complexities of their own data protection will be no match for surveillance capitalism's staggering asymmetries of power.'[326]

Summary

It may appear counterintuitive for a thesis such as this, which places such a focus and emphasis on informational self-determination, to critique those provisions of the GDPR

[324] Susskind (n 18) 352.

[325] It should briefly be acknowledged that the GDPR, in recital 43, does acknowledge the existence of asymmetries of power, where a data subject is required to exercise consent, and suggests that consent should not provide a lawful basis for processing in such circumstances. However, the recital only mentions the power imbalance between a data subject and a public authority, or an employer, and fails to sufficiently address commercial asymmetries of power.

[326] Zuboff (n 25) 482.

which seek to confer precisely this. However, while recognising the importance of provisions which uphold strict requirements of consent and afford valuable rights of control to data subjects, this regulatory progress is rendered inadequate as it does not translate to real change or empowerment for data subjects. This returns us to the discussion of the divergence between the law on the books and the law in action, as previously observed by civil rights advocates and feminist scholars in their respective fields.[327] Landmark legal decisions or legislation, which may appear to be significant and progressive achievements, can become symbolic as the circumstances into which they are enacted prevent any meaningful change for the individuals whose rights they seek to uphold and protect.

For some commentators, these problems fuel a desire to dismiss the value of informational self-determination, or data protection law as a whole; discarding it as simply inadequate or not fit for purpose. It has been described as 'a largely useless Maginot line'[328] or equated to Alfred Hitchcock's character 'Harry'; claiming it is dead and everyone has a different idea of what is to be done with the body.[329] However, it is submitted that such a defeatist attitude is not only unhelpful, but loses track of the value and importance of informational self-determination. If individual data subjects, even when equipped with strong and extensive control rights, are unable to exercise such control due to the overarching and unfair power dynamics of the digital environment, then lawmakers should pursue a regulatory agenda which addresses and confronts those systems of power. In other words, the focus should turn to *informational self-determination in context.*

[327] I am by no means making the claim that the current discussion is as impactful as the work of critical race theorists on civil rights or feminist scholarship on sexual offences. I am merely stating that there is an illuminating parallel between the issues.

[328] Mayer-Schönberger and Cukier (n 24) 16.

[329] Koops (n 256).

# Chapter Four – Informational Self-Determination in Context: Evolving Data Protection Law

> *'Laws and institutions no matter how efficient and well-arranged must be reformed… if they are unjust'*
>
> - John Rawls, A Theory of Justice, 1971[330]

## Introduction

In Chapter Two of this thesis, I endorsed an approach to understanding data protection law as serving two fundamental and related purposes: providing data subjects with the means to exercise control over their personal information; and confronting the problematic power dynamics of the data economy. The GDPR, as discussed above, could be described as offering valuable progress with respect to the former, but failing to properly address the latter.

This chapter will offer an initial outline of some of the emerging proposals and schemes to enhance data subject control, building upon the rights afforded by the GDPR. Thereafter, the focus will turn to the main contribution of the chapter: how to evolve data protection law in pursuit of reforms which directly confront information and power asymmetries. As Frank Pasquale states, 'it is necessary to look at other ways of equalizing the power relationship that surveillance entails.'[331]

In order to achieve this, we should return to, and reconsider, the underlying principles of data protection law, to provide the normative weight and justification for bold

[330] John Rawls, *A Theory of Justice : Original Edition* (Harvard University Press 2020), 3.

[331] Pasquale (n 95) 1016.

and impactful reform. Particular focus will be placed upon the principle of fairness, through a discussion of its rich history as a concept directed at unfair imbalances of power, and the social inequality these systems create. Following this, the chapter will conclude by outlining some prominent proposals for reform, and briefly discussing how a developed understanding of fairness could strengthen these developments.

## Enhancing Informational Self-Determination

The following discussion will focus on two approaches: legal proposals for updating and improving data subject rights (focusing on the right to data portability); and technological or collective mechanisms which encourage or facilitate engagement.

### *Improving data subject rights:*

The potential benefits of the right to data portability has been a topic of much discussion. As explored in the previous chapter, there are concerns and ambiguities regarding the scope and functioning of this right. According to De Hert and others, a restrictive interpretation of this right – as only applying to data explicitly provided by the data subject – creates an approach they call the 'adieu scenario'; limiting the potential of the right.[332] However, an expansive interpretation (including both received and observed data) can contribute to the fusing scenario, whereby data portability plays a key role in a system of 'user-centric platforms of interrelated services.'[333] The overall message being that data portability has great potential to contribute to a developing digital environment which empowers

[332] De Hert and others (n 312) 202.

[333] Ibid 203.

individual data subjects, but significant and expansive interpretation and reform are required.[334]

*Mechanisms to encourage and facilitate engagement:*

In addition to specific legal reforms, a number of forward thinking actors, organisations and data protection advocates have proposed and founded projects with the aim of enhancing individual engagement and control, through technological means. This is an area Shulga-Morskaya dedicates considerable attention to, identifying promising technical developments in pursuit of informational self-determination.[335] One example being 'Solid', which seeks to enable a user to create a decentralised 'personal online data store' (POD), allowing them to control which people and applications have access to it.[336] Another potential development is the concept of Self-Sovereign Identity (SSI) which seeks to utilise blockchain to create a permanent digital identity. For example, the Sovrin project aims to create a 'lifetime portable digital identity that does not depend on any central authority and can never be taken away,'[337] an identity card similar to a passport or wallet which offers the ability to exercise effective control of your online persona outside of the influence of data controllers. These technological solutions are still in the early stages of development, and face significant challenges including concerns over their GDPR compatibility. Nonetheless, the prospect of utilising sophisticated technology to aid in informational self-

[334] The Centre on Regulation in Europe has also published a report outlining proposed improvements to data portability: Jan Krämer, Pierre Senellart and Alexandre de Streel, *Making data portability more effective for the data economy* (Centre on Regulation in Europe, 2020).

[335] Shulga Morskaya (n 8) 11-17.

[336] Steve Lohr, 'He Created the Web. Now He's Out to Remake the Digital World' *The New York Times* (New York, 10 January 2021) <https://www.nytimes.com/2021/01/10/technology/tim-berners-lee-privacy-internet.html> accessed 02 February 2021.

[337] The Sovrin Foundation, *Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust* (White Paper, January 2018, 2018).

determination – as opposed to taking it away – is a welcome development and if these schemes are able to develop successfully and overcome these hurdles, they offer fantastic potential to enhance data subject control.

Another emerging means of facilitating informational self-determination adopts a more collective approach, examples of this include Data Unions,[338] Data Trusts and Data Cooperatives. Data Trusts have garnered significant attention, building upon the centuries old concept of trust law to create a system whereby individual data subjects would entrust or assign rights into a trust, which would be managed by appointed trustees who would be under strict fiduciary duties to these individuals. These trustees would negotiate with those institutions who seek to utilise data to agree to terms governing the use of this data, and monitor compliance with these terms. Data Cooperatives are similar to data trusts, but with more data subject involvement, potentially to be founded to serve a specific purpose which the data subjects may desire to be more involved in such as the use of sensitive data in health or scientific research. A Cooperative has a more positive aim, to achieve some common purpose of its members as opposed to negotiating negative obligations under a Data Trust.[339] The prospect of such collective organisation regarding data rights presents legal difficulties of its own, and some initial work has begun regarding the complexities of these issues, required developments, and barriers to be overcome.[340] Nonetheless, in an environment whereby individuals face great difficulty in exercising effective control on their own, the prospect of collective action could play an important role in subverting the

[338] See the discussion of 'data unions' in Domingos (n 279) 274-275.

[339] Ada Lovelace Institute and UK AI Council, *Exploring legal mechanisms for data stewardship* (Working group, final report, 2021).

[340] See Pinsent Masons, BPE Solicitors and Queen Mary University of London, *Data Trusts: legal and governance considerations* (A Project in Collaboration with the Open Data Institute, 2019).

power asymmetries of the data economy and facilitating a new form of informational self-determination.

In a recent development, the EU Commission appears to be moving in this direction, with the proposed Data Governance Act.[341] The purpose of this proposal is to create a framework which will facilitate data-sharing by increasing trust and strengthening data sharing mechanisms. One aspect particularly relevant in the context of this discussion is the aim to facilitate 'personal data-sharing intermediaries' designed to aid data subjects in exercising their rights. This appears to lay the groundwork for the legal recognition of these collective schemes and technical mechanisms. The proposal outlines the different types of intermediary,[342] the conditions for providing these data services,[343] and mentions the additional criterion of these entities assuming fiduciary duties.[344]

It is important to acknowledge these proposals for legal reform and developing technological mechanisms, as they offer great potential to enable data subjects to engage with the valuable control rights afforded to them by the GDPR. Indeed, some commentators – excited by the prospects of such developments – have called for regulators to step back from existing top-down control, and instead focus all of their energy on encouraging these developments.[345] The schemes described above are encouraging, but both aspects of data

[341] Proposal for a Regulation of the European Parliament and of the Council on European Data Governance COM/2020/767 final (Data Governance Act).

[342] Ibid, art 9.

[343] Ibid, art 11.

[344] Ibid; this is mentioned in the preliminary 'legal basis' section and recital 26.

[345] John Thornhill, 'The people, not governments, should exercise digital sovereignty' *Financial Times* (London).

protection – internal and external to informational self-determination – have a role to play in facilitating an equitable and user-centric digital environment. Data protection law must embark upon an ambitious agenda to address and rectify the significant asymmetries of power which have achieved dominance throughout the data economy. This will require new and more substantial regulations placed upon those who seek to use personal data, but such rules will require a strong normative justification.

## Reforming Data Protection Law: Lawfulness, *Fairness,* and Transparency

### Alternative Approaches to Data Protection

Outside of informational self-determination, or data subject control, there are other views as to the purpose and nature of data protection law. Two common perspectives are: the 'risk-based approach' to data protection; and a focus on 'general principles of fair processing,' placing obligations upon the controller to process data lawfully, fairly and transparently. These perspectives are often viewed as competing visions, and placed in opposition to an understanding of data protection law as concerned with data subject control. However, it is not helpful to view all of these approaches as mutually exclusive. This thesis has stressed the fundamental importance of informational self-determination, while asserting that – given the realities of the data economy – data subject control alone will not solve the problem. A truly comprehensive approach to data protection law should supplement informational self-determination by seeking reform which is external to data subject control. It is therefore worthwhile to consider these alternative views.

The 'risk based approach' requires data controllers to assess the potential risks of their data processing practices, not only to their organisation but also to individual rights.

Gëllert strongly advocates for a risk-based understanding of data protection, as 'a legal framework for the regulation of risks to fundamental rights' or, in other words, 'an attempt to tame the risk of technology.'[346] This approach can be identified in the GDPR, through the responsibilities placed upon data controllers,[347] requirements to implement data protection by design and default[348] and to conduct a data protection impact assessment.[349] Unfortunately, it is beyond the scope of this work to offer a thorough engagement with the risk-based approach. It is however, worth noting as improving compliance through risk-management procedures is likely to play an important role in the development of data protection law.[350] To offer some tentative insights into the future direction of this area of law, this work will focus on the general principles of fair processing.

The rationale and purpose of data protection law is grounded in foundational principles. As previously stated, the GDPR outlines these principles in its early provisions, before comprehensively establishing the rules imposed upon the actors in the data economy. Reforming data protection law to meet the challenges of the data economy is by no means a simple task. However, when seeking potential reform of the regulatory landscape, we should revisit and appeal to these principles to provide normative weight to new legal developments. In this regard, one is reminded of Dworkin's distinction between

[346] Raphaël Gellert, 'Understanding Data Protection as Risk Regulation' (2015) 18 Journal of Internet Law 3; for a more detailed and recent account, see Raphaël Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020).

[347] GDPR, art 24(1).

[348] Ibid, art 25(1).

[349] Ibid, art 35.

[350] For a balanced perspective which emphasises the potential value of data protection law while outlining its potential risks and flaws, see Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' (2018) 9 European Journal Of Risk Regulation: EJRR 502.

rules and principles.[351] This perspective describes the former as 'applicable in an all or nothing fashion,' whereas principles are more general, point towards a social good and may be appealed to in hard cases where our problems are more acute, and the simple and direct application of rules does not lead to a satisfactory outcome.[352] One principle in particular, which has emerged as a focal point in discussions surrounding data protection reform, and will be the main focus of the present account, is the concept of *fairness.*

**The Pursuit of Fairness**

The notion of fairness is undoubtedly at the heart of data protection law, the requirement that data be processed 'fairly' is upheld by Article 8 of the EU Charter.[353] Furthermore, in the GDPR, fairness is placed alongside lawfulness and transparency as fundamental principles relating to processing of personal data.[354] However, despite this heightened importance placed upon fairness, a number of scholars have queried the precise definition of the term in this context.[355] Eskens observes that the GDPR does not offer any further explanation as to the meaning of fairness. Furthermore, when the provisions of the regulation refer to fairness, this is done in a manner which equates it with either lawfulness or transparency.[356] This conflation of fairness and transparency in particular is demonstrated by the opinion of the Article 29 Working Party, 'the fairness principle

[351] Ronald M. Dworkin, 'The Model of Rules' (1967) 35 The University of Chicago Law Review 14.

[352] Ibid, 25.

[353] EU Charter, art 8(2).

[354] GDPR, art 5(1)(a).

[355] Daniel-Mihail Sandru, 'The Fairness Principle in Personal Data Processing' (2020) X Law Review 60.

[356] Eskens outlines that the 'preamble and substantive provisions of the regulation only refer to "lawful and fair" (4 times) or "fair and transparent" (7 times) processing, and nowhere to "fair processing" '. Sarah Eskens, 'Profiling the European Citizen in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should It?' [2016] SSRN Electronic Journal, 27.

specifically requires that personal data should never be collected and processed without the individual actually being made aware of it.'[357] Therefore, it appears that the extent of the fairness requirement is that processing will be deemed 'fair' if it adheres to the legal rules or where the data subject is notified of it, at the expense of any substantive requirement of fairness. This is deeply unfortunate because, as will hopefully be demonstrated in the following discussion, a developed concept of fairness can offer far more to this area of law than an empty and symbolic gesture, or a proxy for lawfulness or transparency.

Fortunately, there is a growing attention towards fairness as a possible foundation for reform. Bygrave observes that the GDPR's principles are sufficiently flexible in order to adapt to meet the challenges of big data analytics, and that fairness 'is especially important in this regard.'[358] In a report on the ethical matters raised by algorithms and AI, the French Data Protection Authority specifically cite the principle of fairness (alongside 'continued attention and vigilance') as a founding principle for future development in this area.[359] Claudi Malgieri, through a linguistic and contextual interpretation of the word 'fairness' in both the official EU languages and the GDPR, draws the conclusion that fairness is effect-based, requiring 'the substantial mitigation of unfair imbalances that create situations of vulnerability' as opposed to merely the formal respect of procedures.[360]

[357] WP29 Opinion 8/2014 on the Recent Developments on the Internet of Things; for another perspective which subsumes fairness under transparency, see Luiz Costa and Yves Poullet, 'Privacy and the regulation of 2012' (2012) 28 The computer law and security report 254, 256.

[358] Bygrave (n 9) 19.

[359] Commission Nationale Informatique & Libertés, *How Can Humans Keep the Upper Hand? The thical matters raised by algorithms and artificial intelligence* (Report on the publid debate led by the French Data Protection Authority (CNIL) as part of the ethical discussion assignment set by the digital republic bill, 2017) 48.

[360] Gianclaudio Malgieri, 'The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation' (Conference on fairness, accountability, and transparency, New York, 2020).

Therefore, fairness is uniquely placed to address the underlying problem with informational self-determination; that it appears unattainable in the face of systemic information and power asymmetries. In order to unlock the normative potential of fairness, further discussion and open debate is required, addressing its conceptual foundations and outlining its substantive effectiveness. The following discussion seeks to contribute to this discourse.

It is true that the idea of fairness can be utilised in more specific circumstances where, for example, an interaction or transaction between two people may be deemed unfair for whatever reason. However, when applied on a wider societal level, 'fairness' acquires a different status and character. This understanding of fairness gained prominence in political philosophy, and this is largely attributed to John Rawls and his seminal work 'A Theory of Justice'.[361] In this account, Rawls is primarily concerned with articulating a conception of social justice, the principles which will determine the structure of social institutions and how fundamental rights, duties and social advantages are distributed; a conception he labels *justice as fairness*.[362] In doing so, he is seeking to elevate 'to a higher level of abstraction' pre-existing theories of the social contract as offered by writes such as Locke, Rousseau and Kant.[363] This perspective is developed through the hypothetical 'original position' under a 'veil of ignorance,' a position where one can observe the state of the social world, with a complete indifference as to their place within it.[364] Rawls asserts that, in such a position, rational beings would assign basic rights and duties and determine the division of social benefits in accordance with two principles: each person would have

[361] Rawls (n 330); defended and partially developed in: John Rawls and Erin Kelly, *Justice as fairness : a restatement* (Harvard University Press 2001).

[362] Rawls (n 330) 7.

[363] Ibid 11.

[364] Ibid 12.

an equal right to the most extensive basic liberties; and social and economic equalities would be arranged to the greatest benefit of the least advantaged (the difference principle) and attached to positions and offices open to all (equality of opportunity).[365]

The Rawlsian approach is useful here because it provides the foundation for a substantive conception of fairness as social justice, of conducting an overall evaluation of society – the organisation of institutions and respect for basic rights and duties – to identify any structural and systematic inequalities and seek to rectify them. The specific principles Rawls develops (particularly the difference principle and equality of opportunity) are more directly concerned with the economic disparities of the late 20th century, seeking to rectify them through distributive justice, and so do not directly translate to the problem at hand. Although, redistribution is not an entirely inapplicable concept, proposals to redistribute the immense wealth acquired by big tech companies, in a just manner, for the overall benefit of society is a worthwhile endeavour, but is really a question of taxation and welfare economics, not data protection. Additionally, the idea of remunerating individuals for the value of their data has attracted a lot of attention,[366] but these arguments miss the 'key point that the… exploitation here is the rendering of our lives as behavioural data for the sake of others' improved control over us.'[367] This is not an issue which can be solved by redistributing the, likely minimal, value of individual data to each user. We should instead

[365] Ibid 60, 83.

[366] See, for example, Will.I.Am, 'We need to own our data as a human right - and be compensated for it' *The Economist* (London, 21 January 2019) <https://www.economist.com/open-future/2019/01/21/we-need-to-own-our-data-as-a-human-right-and-be-compensated-for-it> .

[367] Zuboff, 94; see also the discussion of 'buying our acquiescence' in Shoshana Zuboff, 'The Coup We Are Not Talking About' *The New York Times* (New York, 29 January 2021) <https://www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html> accessed 02 February 2021.

be concerned with achieving a system of governance which recognises and respects individual persons.

Looking beyond redistribution, we should turn to contemporary discussions of social justice which, building upon the work of Rawls and others, have developed an understanding of two spheres of social justice; in addition to redistribution, there is also *justice in recognition*. As opposed to distributive justice, which seeks to rectify socioeconomic inequality through implementing a just distribution of wealth and goods, recognition is concerned with systems which fail to respect the dignity and moral worth of certain individuals or groups. The 'struggle for recognition,' in its various forms, has sought to address the marginalisation and oppression of human beings by social structures which disregard their fundamental desire to be treated with dignity.

Perhaps the most notable discussion of this is an exchange between philosophers Nancy Fraser and Axel Honneth. While the two writers respectfully disagree on the particular contours of, and relationship between, the two spheres of social justice[368] they nonetheless greatly emphasise the importance of justice as recognition. As Honneth claims, 'the recognition of human dignity comprises a central principle of social justice'[369] and such a form of justice should be 'about enabling the formulation of personal identity for all members of society.'[370]

---

[368] Fraser seeks to maintain a distinction between the two spheres while Honneth contends that recognition is primary and central, and that ideas such as distribution are 'phenomenologically secondary'. See: Nancy Fraser and Axel Honneth, *Redistribution or recognition? : a political-philosophical exchange* (Verso 2003).

[369] Axel Honneth, 'Recognition and justice outline of a plural theory of justice' (2004) 47 Acta sociologica 351, 352.

[370] Ibid, 356; see also Nancy Fraser, *Justice interruptus : critical reflections on the "postsocialist" condition* (Routledge 1997), 11-32.

This idea of recognition can be traced back to philosophers such as Georg Wilhelm Friedrich Hegel and Immanuel Kant. The concept is central to the Hegelian school of thought, as the reciprocal recognition of one another as self-conscious subjects, in addition to self-recognition, is essential to the acquisition of self-consciousness and development of one's personality.[371] Other writers have built upon Hegel's ideas to emphasise the importance of recognition in a way which is not quite so impenetrable. Honneth is a loyal Hegelian and the account cited above adopts a distinctly Hegelian perspective.[372] In addition, Charles Taylor asserts that a lack of recognition can place a person in 'a reduced mode of being' and that 'due recognition is not a courtesy but a vital human need.'[373] Furthermore, recognition can be seen at the very heart of Kantian morality. For instance, with the second formulation of Kant's categorical imperative, 'act in such a way that you treat humanity, whether in your own person or in the person of any other, never simply as a means but always at the same time as an end.'[374]

If we refer to the discussion of big data and surveillance capitalism in the early sections of this thesis. We can recount that the utilisation of big data analysis by corporate entities places them in a unique and unprecedented position, with the ability to exert unforeseen control and domination over data subjects in pursuit of commercial ends. This situation is,

---

[371] See generally, Georg Wilhelm Friedrich Hegel, Allen W. Wood and H. B. Nisbet, *Elements of the philosophy of right* (Cambridge University Press 1991); Georg Wilhelm Friedrich Hegel, *The Phenomenology of Spirit* (Cambridge University Press Terry Pinkard tr ed, 2017).

[372] Honneth (n 369) 354.

[373] Charles Taylor, *Multiculturalism and 'The Politics of Recognition'* (Princeton University Press 1992), 25.

[374] Immanuel Kant, 'Groundwork of The metaphysics of morals (1785)' in Mary J. Gregor (ed), *Practical Philosophy* (Cambridge University Press 1996) 78-79.

inherently, a problem of justice in recognition. Surveillance capitalism has created a system and structure which, if left unchecked and unguided by a strong ethical framework, will create and entrench deep inequalities of recognition at the great expense of the individual data subject. Justice in recognition has typically been utilised against the oppression or subjugation of certain groups; on the basis of classifications such as race, gender and sexuality. The new form of injustice we are witnessing presents an unprecedented and overarching division; between those who process data and those whose data is processed. This 'division of learning' also has the potential to exacerbate pre-existing cultural divides, through – for example – biased algorithms. The very idea of acquiring a substantial wealth of information pertaining to an individual, in order to control and manipulate their thoughts and actions in pursuit of your own agenda, is in direct opposition to the Kantian maxim which prohibits treating the humanity of others simply as a means to an end. The expansion of private surveillance techniques to control and manipulate individuals and the prospects of unfair treatment and discrimination are all consequences of a systemic failure to recognise the dignity of individuals and groups.

As Bygrave states, 'fairness has independent work to do'[375] in order to realise its full potential. It is submitted here that a reconsideration of the foundations and rich history of fairness can offer a valuable contribution and provide normative weight to the principle as a driving force for reform in this area. In particular, the notion of fairness as social justice in recognition appears particularly valuable in pursuing regulations which seek to confront information and power asymmetries to respect the dignity and moral status of data subjects. There is, undoubtedly, a wealth of further possible insights to be gained from the scholars

[375] Bygrave (n 9) 19.

cited above. At the very least, I hope to have offered a valid contribution to discussions regarding the development of the fairness principle in data protection law.

**Potential for Reform**

In order to extend the claims made in this chapter beyond a purely conceptual discussion placing emphasis on a developed notion of fairness, this section seeks to offer some indications of the potential reforms in this area. Due to the limitations of this thesis, it is not possible to offer a lengthy and critical engagement with these proposals, the aim is simply to outline the emerging ideas, and offer some indications of the role a developed principle of fairness could play in these developments.

In order to address the power asymmetry between the data controller and data subject, it is submitted that stronger and more specific ethical duties must be placed upon data controllers, which are imposed irrespective of data subject control. Data controllers should not be able to escape many of their obligations by acquiring the consent of the data subject. Evolving such a regulatory landscape will require extensive deliberation, and a greater understanding of the technological complexities involved in the processing of data; such a process will be a lengthy and perhaps never-ending task.[376] Nonetheless, a developed principle of fairness – directly addressing overarching power asymmetries – can provide a strong conceptual foundation for such developments. In other words, fairness can concretely justify and indeed oblige 'the adoption of ethical data practices and

[376] For a discussion of the kind of ethical framework which could be required of data controllers, see Martin Abrams, 'Applying Ethics When Using Data beyond Individuals' Understanding' in Evan Selinger, Jules Polonetsky and Omer Tene (eds), *The Cambridge Handbook of Consumer Privacy* (Cambridge, United Kingdom 2018).

standardization mechanisms that effectively incorporate broader social rights-based considerations.'[377]

In addition to applying more stringent ethical duties upon data controllers, the principle of fairness can enhance the risk-based approach to data protection; in particular the requirement to conduct a data protection impact assessment. As some writers have observed, it is unclear how the principle of fairness applies to this requirement and various guidance documents on conducting these assessments do not reference fairness in any clear or substantial way.[378] The paper asserts that a developed principle of fairness could significantly improve the effectiveness of these mechanisms. Embedding considerations of fairness into these procedures could develop them from minimal and routine tick-box compliance to a more meaningful process whereby data controllers acknowledge their unique position, and take every step necessary to ensure their actions do not impede upon fundamental rights. Furthermore, the potential for fairness to combat algorithmic discrimination and bias has become a topic of increasing consideration.[379]

Moreover, discussions concerned with addressing information and power asymmetries have increasingly focused upon developing the relationship between data

[377] Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130.

[378] Atoosa Kasirzadeh and Damian Clifford, 'Fairness and Data Protection Impact Assessments' (Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society (AIES '21), New York, 19-21 May 2021).

[379] See, generally Michael Butterworth, 'The ICO and artificial intelligence: The role of fairness in the GDPR framework' 34 The computer law and security report 257; Philipp Hacker, 'Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law' (Cambridge) 55 Common Market Law Review 1143.

protection law, competition law, and consumer law.[380] Competition law is aligned with data protection as its concern with abuses of dominant market position reflect concerns in data protection law over the power acquired by certain data controllers. In other words, both areas of law 'share foundational concerns and remedial approaches… they seek to mitigate unfairness by imposing obligations on those with information or market power and giving rise to those with less power.'[381] It has also been observed that consumer law and data protection law 'could apply in parallel'[382] and the former could enhance the latter in areas such as addressing unfair terms, unfair practices, and consumer vulnerability.[383] Establishing a coherent and comprehensive unified approach across these areas of law is a formidable task, but also offers worthwhile and exciting possibilities for future research and reform. The potential role of fairness in this regard has been observed. Graef and others, in an account which extensively explores the prospects for collaboration across these areas, emphasises fairness as 'an overarching principle that plays a role in each of these regimes… [and] can act as the normative underpinning for such more coherent approaches.'[384]

I am acutely aware that these discussions remain preliminary and somewhat abstract, as the specific ways through which fairness can be integrated into, and enhance,

[380] Discussions in this regard started with the publication of EDPS Preliminary Opinion of 26 March 2014 on 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy'.

[381] Christian D'Cunha, 'Best of frenemies? Reflections on privacy and competition four years after the EDPS Preliminary Opinion' (2018) 8 International Data Privacy Law 253, 254.

[382] Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, ''The perfect match? A closer look at the relationship between EU consumer law and data protection law' (2017) 54 Common Market Law Review 1427, 1429.

[383] Ibid 1435-1459.

[384] Inge Graef, Damian Clifford and Peggy Valcke, 'Fairness and enforcement: bridging competition, data protection, and consumer law' (2018) 8 International Data Privacy Law 200, 223.

these reforms are not fully developed. Such a prospect does, however, offer a promising avenue for future debate and research. In addition, other values and principles – already integral to data protection – will have a role to play. For instance, a fairer system will seek to improve trust, and require greater transparency and accountability. To conclude, the overall purpose of this discussion has been to assert that fairness offers great and exciting potential to facilitate a more ethically stringent, equitable, and balanced digital environment – and hopefully - an environment in which data subjects are able to exercise true informational self-determination.

# Conclusion

*'Let there be a digital future, but let it be a human future first'*

- Shoshana Zuboff, *The Age of Surveillance Capitalism,* 2019[385]

In 1989, Tim Berners-Lee wrote a paper titled 'Information Management: A Proposal', which laid the foundations for what would become the World Wide Web. In an interview almost 30 years later, the computer scientist expressed his devastation towards what his creation had become. In doing so, he recounted the exciting early days of the internet – its democratising potential and capacity for creativity, collaboration, and progress – before stating, 'that feeling of individual control, that empowerment, is something we've lost.'[386] This early optimism and excitement was predicated upon the belief that the greatly enhanced interconnectivity of the internet would serve us, and vastly improve our lives. Obviously, in many ways it has, but recently we have witnessed the a trend which goes in the opposite direction. Online activity and the flow of information, particularly personal information, has been monopolised by powerful corporations. These entities now have the power to utilise this data in ways which have a profound impact upon our lives, in a manner we are not aware of, and do not truly understand. This phenomenon can be aptly described as the, deeply regrettable, loss of our right to informational self-determination. The GFCC, and its ruling in 1983 concerning invasive government surveillance, articulated a concept which is strikingly relevant to the underlying problems of the information age. This thesis, seeking to explore the legal response to these circumstances, in the areas of privacy and data protection, has therefore placed great emphasis upon this notion.

---

[385] Zuboff (n 25) 522.

[386] Katrina Brooker, ''I was devastated': Tim Berners-Lee, the man who created the world wide web, has some regrets' (*Vanity Fair*, 01 July 2018) <https://www.vanityfair.com/news/2018/07/the-man-who-created-the-world-wide-web-has-some-regrets> accessed 10 July 2021.

This problem has only emerged recently and, as such, we are only beginning to grapple with the complexities and implications of it. Chapter One of began with a comprehensive discussion of this emerging threat, and its overwhelming potential to reconstruct social dynamics at the expense of fundamental rights and freedoms of individual persons. The problems arise from the actions of a number of powerful companies – described as 'surveillance capitalists' – utilising an approach to data collection and statistical analysis which has been labelled 'big data.' This has allowed them to acquire a new, unique and unprecedented form of power, analysing and processing their vast stores of personal information to predict, control, and manipulate individuals in search of greater profits. The ubiquity and invasiveness of the innovative technological devices these companies produce, and our ever-increasing reliance upon them, is emblematic of their persistent desire to continue amassing information in pursuit of more effective means of control.

When many people observe these developments on a surface level, they often label them as an 'invasion of privacy.' However, as discussed in the second part of the first chapter, relying solely on the right to privacy may not offer a sufficient solution. Privacy, while contested and ambiguous, generally delimits a zone of non-interference, a private sphere, on the basis of maintaining desires toward – for example – seclusion, solutide, intimacy or dignity. While we should approach privacy with a pragmatic perspective, deploying these values in a context-dependent manner, privacy's limitations render it unable to offer sufficient protection to individuals in response to surveillance capitalism. Just as Warren and Brandeis, advocating in 1890 for the recognition of the right to privacy, observed that the preexisting law of defamation rests upon a principle which 'covers… a

radically different class of effects from those for which attention is now asked,'[387] data protection law requires another shift in focus.

This leads us to Chapter Two, which introduced the right to informational self-determination as an concept of invaluable importance in this regard, while also tracking the emergence of data protection as a fundamental right in Europe. As explored extensively in this chapter, unlocking the promising potential of data protection relies upon recognising its distinct independent value outside of privacy, due to its concern with securing data subject control and addressing the fundamental power imbalances of the data economy. The importance of informational self-determination within data protection is therefore revealed, as the functions of data protection work both internally and externally to informational self-determination.

However, the above analysis does not represent a settled consensus regarding the character and purpose of data protection. This is most pertinently demonstrated by the jurisprudence of the ECtHR and CJEU. Both courts have sought to address the problems we are concerned with and have made some worthwhile progress. Particularly the CJEU, which has made landmark, high-profile rulings: maintaining a strict standard of consent; upholding fundamental rights against economic interests; and preventing excessive and unjustified surveillance regarding international data transfers and state data collection. However, the underlying reasoning afforded by the two courts consistently conflates the two fundamental rights of privacy and data protection. For those who wish to see data

[387] Warren and Brandeis (n 82) 197.

protection sufficiently developed to confront the problematic aspects of the information age, this is an inadequate state of affairs.

The introduction of the GDPR in 2016 offered great hope to many data protection advocates. Indeed, on the topic of informational self-determination in particular, the regulation is a very important and progressive legal instrument. Data subject control takes up an important role, as the legislation maintains a strict standard of consent and affords individuals a range of useful rights to manage the processing of their personal information. However, an analysis of the practical implementation and exercisability (or lack thereof) of these rights is a sobering project. There exists a gaping divergence between the law on the books and the law in action. This was demonstrated by focusing specifically on the provisions regarding consent and the rights to erasure and data portability.

However, we would be gravely mistaken to dismiss the value of informational self-determination; and there are many proposed legal reforms and organisational endeavours which seek to enhance and improve data subject control. Furthermore, if the environment in which data subjects are expected to exercise informational self-determination currently renders such a prospect unfeasible, then focus should turn to the wider overarching problems. This is the primary focus of Chapter Four, seeking legal reforms which confront the information asymmetries and uneven power dynamics created by commercial data processing. This section advocated for a reconsideration and further discussion of the foundational principles of data protection law. It is submitted that the principle of fairness – considerably under-developed in this context – offers great promise. Fairness can be understood as directly concerned with societal imbalances of power, and such a conception – particularly of fairness as social justice in recognition – can offer substantial normative

weight behind effective and wide-reaching reform. This discussion concluded with a brief outline of some proposals for such reform, and indicated the potential contribution of a developed principle of fairness in this regard.

The problem this thesis has sought to address is not a technological problem, it is a social problem exacerbated by technology. Thankfully, we have well-established institutions and laws capable of responding to this threat; and the EU appears to be leading in this response. However, as these developments continue to advance at a seemingly exponential rate, our norms, standards and rules need to adapt. With bold and reasoned progress and reform, we can create an environment in which individuals are able to take control of their personal information and, by extension, their lives.

# Bibliography

## Books


Bauman Z, *Liquid modernity* (Polity Press 2000)

Costa M, Peers S and Steiner J, *Steiner & Woods EU law* (14th edition edn, Oxford University Press 2020)

Domingos P, *The master algorithm : how the quest for the ultimate learning machine will remake our world* (Allen Lane 2015)

Durkheim E and Lukes S, *Durkheim: The Division of Labour in Society* (2nd edn, Palgrave Macmillan 2013)

Europe Co, *Handbook on European data protection law 2018 edition* (Luxembourg : Publications Office 2018)

Floridi L, *The 4th revolution : how the infosphere is reshaping human reality* (Oxford University Press 2014)

Foucault M, *'Society Must Be Defended' Lectures at the Collège de France 1975-76* (Bertani M and Fontana A eds, Macey D tr, Picador, New York 2003)

——, *Discipline and punish: the birth of the prison* (Penguin 2019)

Fraser N, *Justice interruptus : critical reflections on the "postsocialist" condition* (Routledge 1997)

Fraser N and Honneth A, *Redistribution or recognition? : a political-philosophical exchange* (Verso 2003)

Gellert R, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020)

Gutwirth S, *Privacy and the information age* (Rowman & Littlefield 2002)

Hegel GWF, *The Phenomenology of Spirit* (Terry Pinkard tr CUP ed, 2017)

Hegel GWF, Wood AW and Nisbet HB, *Elements of the philosophy of right* (Cambridge University Press 1991)

Inness JC, *Privacy, intimacy, and isolation* (Oxford University Press 1992)

Lessig L, *Code : and other laws of cyberspace* (Basic Books 1999)

Mayer-Schönberger V and Cukier K, *Big data : a revolution that will transform how we live, work and think* (New and expanded edn, John Murray 2017)

Miller AR, *The assault on privacy : computers, data banks, and dossiers* (University of Michigan Press 1971)

O'Neil C, *Weapons of math destruction : how big data increases inequality and threatens democracy* (Penguin Books 2017)

Packard V, *The naked society* (Penguin 1966)

Purtova NN, *Property rights in personal data: A European perspective* (Prins C and others eds, Uitgeverij BOXPress, Oisterwijk 2011)

Rawls J, *A Theory of Justice : Original Edition* (Harvard University Press 2020)

Rawls J and Kelly E, *Justice as fairness : a restatement* (Harvard University Press 2001)

Rule JB, *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience* (Oxford University Press 2009)

Susskind J, *Future politics : living together in a world transformed by tech* (Oxford University Press 2020)

Susskind RE and Susskind D, *The future of the professions : how technology will transform the work of human experts* (First edn, Oxford University Press 2015)

Taylor C, *Multiculturalism and 'The Politics of Recognition'* (Princeton University Press 1992)

Véliz C, *Privacy is power : why and how you should take back control of your data* (Bantam Press 2020)

Wacks R, *Privacy : a very short introduction* (Second edn, Oxford University Press 2015)

Westin AF, *Privacy and freedom* (1st edn, Atheneum 1968)

Williamson B, *Big data in education : the digital future of learning, policy and practice* (SAGE Publications Ltd. 2017)

Wittgenstein L, *Philosophical Investigations* (Anscombe GEM tr, Basil Blackwell 1958)

Zhang Z and Li J, *Big data mining for climate change* (Elsevier 2020)

Zuboff S, *The age of surveillance capitalism: the fight for a human future at the new frontier of power* (Profile Books 2019)

Conference Papers

Kasirzadeh A and Clifford D, 'Fairness and Data Protection Impact Assessments' (Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society (AIES '21), New York, 19-21 May 2021)

Malgieri G, 'The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation' (Conference on fairness, accountability, and transparency, New York, 2020)

Mangini V, Tal I and Moldovan A-N, 'An empirical study on the impact of GDPR and right to be forgotten - organisations and users perspective' (Proceedings of the 15th International Conference on Availability, Reliability and Security)

Shulga Morskaya T, 'Protection of Personal Data through Implementation of the Right to Informational Self-Determination: Identifying Opportunities and Pitfalls' (2019 Annual GigaNet Symposium, Berlin, 25 November 2019)

Contributions to Edited Books

Abrams M, 'Applying Ethics When Using Data beyond Individuals' Understanding' in Selinger E, Polonetsky J and Tene O (eds), *The Cambridge Handbook of Consumer Privacy* (Cambridge, United Kingdom 2018)

Bullock EC, 'Valid Consent' in Müller A and Schaber P (eds), *The Routledge handbook of the ethics of consent* (Routledge 2018)

Custers B and others, 'Consent and Privacy' in Müller A and Schaber P (eds), *The Routledge handbook of the ethics of consent* (Routledge 2018)

De Hert P and Gutwirth S, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in Claes E, Duff A and Gutwirth S (eds), *Privacy and the criminal aw* (Intersentia 2006)

Gandy Jr OH, 'Statistical surveillance: Remote sensing in the digital age' in Ball K, Haggerty K and Lyon D (eds), *Routledge Handbook of Surveillance Studies* (London, Routledge 2012)

Gutwirth S and De Hert P, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action' in Gutwirth S and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009)

Hume D, 'Of the first principles of government' in Haakonssen K (ed), *Hume: Political Essays* (Cambridge University Press 1994)

Hurd HM, 'The Normative Force of Consent' in Müller A and Schaber P (eds), *The Routledge handbook of the ethics of consent* (Routledge 2018)

Kant I, 'Groundwork of The metaphysics of morals (1785)' in Gregor MJ (ed), *Practical Philosophy* (Cambridge University Press 1996)

Koch F, 'Consent as a Normative Power' in Müller A and Schaber P (eds), *The Routledge handbook of the ethics of consent* (Routledge 2018)

Kranenborg H, 'Protection of Personal Data' in Peers S and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing 2014)

Lyon D, 'Surveillance as social sorting: computer codes and mobile bodies' in Lyon D (ed), *Surveillance as social sorting: privacy, risk and discrimination* (Taylor & Francis Group 2002)

Mayer-Schönberger V, 'Generational development of data protection in Europe' in *Technology and privacy: the new landscape* (MIT Press 1997)

Rouvroy A and Poullet Y, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Gutwirth S and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009)

Terwangne Cd, 'The right to be forgotten and the informational autonomy in the digital environment' in Ghezzi A, Pereira ÂG and Vesnić-Alujević L (eds), *The Ethics of Memory in a Digital Age Palgrave Macmillan Memory Studies* (Palgrave Macmillan 2013)

Edited Books

Peers S and others (eds), *The EU Charter of Fundamental Rights : a commentary* (Hart Publishing 2014)

Journal Articles

Khaitan T and Steel S, 'Theorising Areas of Law' (2019) <https://ssrn.com/abstract=3464432> accessed 23 October 2020

Turner S and others, 'The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment' New Media & Society <https://doi.org/10.1177/1461444820934033> accessed 28 March 2021

Bell DA, Jr., 'Brown v. Board of Education and the Interest-Convergence Dilemma' (1980) 93 Harvard Law Review 518

Bloustein EJ, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 New York University Law Review 962

Butterworth M, 'The ICO and artificial intelligence: The role of fairness in the GDPR framework' 34 The computer law and security report 257

Bygrave LA, 'The place of privacy in data protection law' (2001) 7 University of New South Wales Law Journal forum 26

Clifford D and Ausloos J, 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130

Cohen JE, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 Stanford Law Review 1373

Costa L and Poullet Y, 'Privacy and the regulation of 2012' (2012) 28 The computer law and security report 254

Cowan S, 'Sense and Sensibilities: A Feminist Critique of Legal Interventions against Sexual Violence' (2019) 23 Edinburgh Law Review 22

D'Cunha C, ‘Best of frenemies? Reflections on privacy and competition four years after the EDPS Preliminary Opinion’ (2018) 8 International Data Privacy Law 253

De Hert P and others, ‘The right to data portability in the GDPR: Towards user-centric interoperability of digital services’ (2018) 34 The computer law and security report 193

Deleuze G, ‘Postscript on the Societies of Control’ (1992) 59 The MIT Press 3

Diebold FX, ‘On the Origin(s) and Development of the Term 'Big Data'’ [2012] SSRN Electronic Journal

Dudziak ML, ‘Brown as a Cold War Case’ (2004) 91 The Journal of American History 32

Duncan N, ‘Defining and describing what we do: doctrinal legal research’ 17 Deakin Law Review 83

Dworkin RM, ‘The Model of Rules’ (1967) 35 The University of Chicago Law Review 14

Eskens S, ‘Profiling the European Citizen in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should It?’ [2016] SSRN Electronic Journal

Favaretto M, De Clercq E and Elger BS, ‘Big Data and discrimination: perils, promises and solutions. A systematic review.(Research)(Report)’ (2019) 6 Journal of Big Data

Gellert R, ‘Understanding Data Protection as Risk Regulation’ (2015) 18 Journal of Internet Law 3

Graef I, Clifford D and Valcke P, ‘Fairness and enforcement: bridging competition, data protection, and consumer law’ (2018) 8 International Data Privacy Law 200

Hacker P, ‘Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law’ (Cambridge) 55 Common Market Law Review 1143

Helberger N, Borgesius FZ and Reyna A, ‘'The perfect match? A closer look at the relationship between EU consumer law and data protection law’ (2017) 54 Common Market Law Review 1427

Honneth A, ‘Recognition and justice outline of a plural theory of justice’ (2004) 47 Acta sociologica 351

Kitchin R and McArdle G, ‘What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets’ (2016) 3 Big data & society

Kokott J and Sobotta C, ‘The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR’ (2013) 3 International Data Privacy Law 222

Koops B-J, ‘The trouble with European data protection law’ (2014) 4 International Data Privacy Law 250

Li W, ‘A tale of two rights: exploring the potential conflict between right to data portability and right to be forgotten under the General Data Protection Regulation’ (2018) 8 International Data Privacy Law 309

Lynskey O, ‘Deconstructing Data Protection: The ‘Added-Value’ of a Right to Data Protection in the EU Legal Order’ (2014) 63 International and Comparative Law Quarterly 569

Lyon D, ‘Surveillance, Snowden, and Big Data: Capacities, consequences, critique’ (2014) 1 Big data & society

Mark W, ‘The Computer for the 21st Century’ (1991) 265 Scientific American 94

McCrudden C, ‘Legal research and the social sciences.(United Kingdom)’ 122 Law Quarterly Review 632

McDonald AM and Cranor LF, ‘The Cost of Reading Privacy Policies’ (2008) 4 A Journal of Law and Policy for the Information Society 543

Obermeyer Z and Emanuel EJ, ‘Predicting the Future — Big Data, Machine Learning, and Clinical Medicine’ (2016) 375 The New England journal of medicine 1216

Pasquale FA, ‘Privacy, antitrust, and power’ (2013) 20 George Mason Law Review 1009

Penney J, ‘Chilling Effects: Online Surveillance and Wikipedia Use’ (2016) 31 Berkeley Technology Law Journal 117

Politou E and others, ‘Backups and the right to be forgotten in the GDPR: An uneasy relationship’ (2018) 34 The computer law and security report 1247

Poullet Y, ‘Is the general data protection regulation the solution?’ (2018) 34 The computer law and security report 773

Pound R, ‘Law in Books and Law in Action’ (1910) 44 American law review 12

Prosser WL, ‘Privacy’ (1960) 48 California Law Review 383

Quelle C, ‘Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach’ (2018) 9 European Journal Of Risk Regulation: EJRR 502

Sandru D-M, ‘The Fairness Principle in Personal Data Processing’ (2020) X Law Review 60

Schauer F, ‘Fear, Risk and the First Amendment: Unraveling the Chilling Effect’ (1978) 58 Boston University Law Review 685

Solove D, ‘Conceptualizing Privacy’ (2002) 90 California Law Review 1087

——, ‘"I've Got Nothing to Hide" and Other Misunderstandings of Privacy’ (2007) 44 The San Diego Law Review 745

—, ‘The End of Privacy?’ (2008) 299 Scientific American 100

Urquhart L, Sailaja N and McAuley D, ‘Realising the right to data portability for the domestic Internet of things’ (2018) 22 Personal and Ubiquitous Computing 317

van Dijck J, ‘Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology’ (2014) 12 Surveillance & Society 197

Wachter S, ‘Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR’ (2018) 34 Computer Law and Security Review

Walklate S, ‘What is to be Done About Violence Against Women?’ (2008) 48 The British Journal of Criminology 39

Warren SD and Brandeis LD, ‘The Right to Privacy’ (1890) 4 Harvard Law Review 193

West SM, ‘Data Capitalism: Redefining the Logics of Surveillance and Privacy’ (2019) 58 Business & society 20

Widjaja AE and others, ‘Understanding users' willingness to put their personal information on the personal cloud-based storage applications: An empirical study’ (2019) 91 Computers in human behavior 167

Wong J and Henderson T, ‘The right to data portability in practice: exploring the implications of the technologically neutral GDPR’ (2019) 9 International Data Privacy Law 173

Yeung K, ‘'Hypernudge': Big Data as a mode of regulation by design’ (2017) 20 Information, communication & society 118

Zaeem RN and Barber KS, ‘The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise’ (2020) 12 ACM Transactions on Management Information Systems 1

Zarsky TZ, ‘Incompatible: The GDPR in the Age of Big Data.(General Data Protection Regulation)’ (2017) 47 Seton Hall Law Review 995

Newspaper Articles

‘The world’s most valuable resource is no longer oil, but data’ *The Economist* (London, 6 May 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>

Arthur C, ‘Tech giants may be huge, but nothing matches big data’ *The Guardian* (London, 23 August 2013) 6

Astor M, ‘Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared’ *The New York Times* (New York, 25 July 2017) <https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html> accessed 7 June 2021

Godkin EL, 'The Rights of the Citizen, IV—To His Own Reputation' *Scribner's Magazine* (New York, July-Dec 1890) 65

Harford T, 'Big data: are we making a big mistake?' *Financial Times* (London, 28 March 2014) <https://www.ft.com/content/21a6e7d8-b479-11e3-a09a-00144feabdc0> accessed 16 April 2021

Johnson B, 'Privacy no longer a social norm, says Facebook founder' *The Guardian* (London, 11 January 2010) <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy> accessed 29/02/2021

Lohr S, 'He Created the Web. Now He's Out to Remake the Digital World' *The New York Times* (New York, 10 January 2021) <https://www.nytimes.com/2021/01/10/technology/tim-berners-lee-privacy-internet.html> accessed 02 February 2021

McGee P, 'Musk-backed Neuralink unveils upgraded brain-implant technology' *Financial Times* (London, 29 August 2020)

Polacheck M, '5 companies that want to track your emotions' *Fortune* (New York City, 22 August 2020) <https://fortune.com/2020/08/22/emotion-sensing-tracking-technology-apps/> accessed 1 June 2021

Preston A, 'The death of privacy' *The Guardian* (London, 3 August 2014) <https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston> accessed 30 February 2021

Thornhill J, 'The people, not governments, should exercise digital sovereignty' *Financial Times* (London)

Will.I.Am, 'We need to own our data as a human right - and be compensated for it' *The Economist* (London, 21 January 2019) <https://www.economist.com/open-future/2019/01/21/we-need-to-own-our-data-as-a-human-right-and-be-compensated-for-it>

Wu T, 'The Tyranny of Convenience' *The New York Times* (New York City, 16 February 2018) <https://www.nytimes.com/2018/02/16/opinion/sunday/tyranny-convenience.html> accessed 09 December 2020

Zuboff S, 'The Coup We Are Not Talking About' *The New York Times* (New York, 29 January 2021) <https://www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html> accessed 02 February 2021

Reports and Research Papers

Bygrave L, *Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions* (University of Oslo Faculty of Law Research Paper No 2020-35, 2020)

Druschel P, Backes M and Tirtea R, *The right to be forgotten - between expectations and practice* (European Network and Information Security, 2012)

Foundation TS, *Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust* (White Paper, January 2018, 2018)

IDC, *Always Connected: How Smartphones and Social Keep us Engaged* (An IDC Research Report, Sponsored by Facebook, 2013)

Institute AL and Council UA, *Exploring legal mechanisms for data stewardship* (Working group, final report, 2021)

Krämer J, Senellart P and Streel Ad, *Making data portability more effective for the data economy* (Centre on Regulation in Europe, 2020)

Libertés CNI, *How Can Humans Keep the Upper Hand? The thical matters raised by algorithms and artificial intelligence* (Report on the publid debate led by the French Data Protection Authority (CNIL) as part of the ethical discussion assignment set by the digital republic bill, 2017)

Masons P, Solicitors B and London QMUo, *Data Trusts: legal and governance considerations* (A Project in Collaboration with the Open Data Institute, 2019)

Proposals, Drafts and Opinions

Draft Charter of the Fundamental Rights of the European Union (05 May 2000) https://www.europarl.europa.eu/charter/activities/docs/pdf/convent28_en.pdf

EDPS Preliminary Opinion of 26 March 2014 on 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy'

WP29 Opinion 8/2014 on the Recent Developments on the Internet of Things

EDPS Opinion 3/2015 of 27 July 2015, Europe's big opportunity: EDPS recommendations on the EU's options for data protection reform

Proposal for a Regulation of the European Parliament and of the Council on European Data Governance COM/2020/767 final (Data Governance Act)

Theses

Filipová P, 'The impact of the CJEU case law on the interpretation of the fundamental rights to privacy and data protection' (Master's Thesis, Charles University 2017)

Web Pages and Blogs

'Data Protection Day: 40 years of Convention 108' (*Council of Europe*, 27 January 2021) <https://www.coe.int/en/web/portal/-/data-protection-day-40-years-of-convention-108> accessed 14 April 2021

Brooker K, ''I was devastated': Tim Berners-Lee, the man who created the world wide web, has some regrets' (*Vanity Fair*, 01 July 2018) <https://www.vanityfair.com/news/2018/07/the-man-who-created-the-world-wide-web-has-some-regrets> accessed 10 July 2021

Callaway E, '"It will change everything": DeepMind's AI makes gigantic leap in solving protein structures' (*nature*, 30 November 2020) <https://www.nature.com/articles/d41586-020-03348-4> accessed 01 February 2021

DeCew J, 'Privacy' (*The Stanford Encyclopedia of Philosophy*, Spring 2018 Edition) <https://plato.stanford.edu/archives/spr2018/entries/privacy/> accessed 2 February 2021

Grauer Y, 'Staggering variety of clandestine trackers found in popular android apps' (*The Intercept*, 24 November 2017) <https://theintercept.com/2017/11/24/staggering-variety-of-clandestine-trackers-found-in-popular-android-apps/> accessed 7 May 2021

Kerr I and Earle J, 'Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy' (*Stanford Law Review*, September 2013) <https://www.stanfordlawreview.org/online/privacy-and-big-data-prediction-preemption-presumption/> accessed 01 February 2021

Klosowski T, 'Facial Recognition Is Everywhere. Here's What We Can Do About It.' (*Wirecutter*, 15 July 2020) <https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/> accessed 25 April 2021

Leibowitz J, 'Introductory remarks at the FTC Roundtable' (*FTC*, 7 December 2009) <https://www.ftc.gov/public-statements/2009/12/introductory-remarks-ftc-privacy-roundtable> accessed 14 April 2021

Salinas S and Balakrishnan A, 'Mark Zuckerberg has been talking and apologising about privacy since 2003 - here's a reminder of what he's said' (*CNBC*, 19 December 2018) <https://www.cnbc.com/2018/12/19/facebook-ceo-mark-zuckerberg-privacy-apologies.html> accessed 01 July 2021

Sharma C, 'Correcting the IoT History' (*Chetan Sharma Consulting*, 19 June 2020) <http://www.chetansharma.com/correcting-the-iot-history/> accessed 6 May 2021

Shaw J, 'The Watchers: Assaults on Privacy in America' (*Harvard Magazine*, January 2017) <https://www.harvardmagazine.com/2017/01/the-watchers> accessed 13 April 2021

Stanley J, 'The Potential Chilling Effects of Big Data' (*American Civil Liberties Union*, 30 April 2012) <https://www.aclu.org/blog/privacy-technology/consumer-privacy/potential-chilling-effects-big-data> accessed 13 April 2021