UNIVERSITY *of the*
WESTERN CAPE

FACULTY OF LAW

DEPARTMENT OF MERCANTILE LAW

PROPERTY RIGHTS IN PERSONAL INFORMATION: A SOUTH AFRICAN PERSPECTIVE

A thesis submitted in fulfilment of the requirements for the degree Doctor Legum (LLD)

By

MARLIN LOWELL FRANSMAN

(Student Number: 4070889)

UNIVERSITY *of the*
WESTERN CAPE

Supervisor: Prof. Fareed Moosa

Co-supervisor: Prof. Vivienne Lawack

JUNE 2024

https://uwcscholar.uwc.ac.za/home

TABLE OF CONTENTS

Declaration iii

Acknowledgements iv

Abstract v

Keywords / Terms vi

Abbreviations vii

Chapter One: Introduction and rationale for the study 10

Chapter Two: Technological developments and the privacy challenges posed by new technologies 29

Chapter Three: Assessing South Africa's data protection regime in light of current personal data processing practices 61

Chapter Four: The propertisation of personal information from a United States perspective 95

Chapter Five: The European data protection framework and the personal information trade 142

Chapter Six: Expanding on the concept of constitutional property with specific reference to personal information 188

Chapter Seven: Conclusion and Recommendations 212

Appendix: Draft Personal Information Commodities Bill, 2024 226

Bibliography 236

UNIVERSITY of the WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

DECLARATION

I, Marlin Lowell Fransman, declare that the thesis titled 'Property Rights in Personal Information: A South African Perspective' is my own work, that it has not been written by artificial intelligence, that any use of artificial intelligence accords with the ethical norms and standards for research at the University of the Western Cape, and that this thesis has not been submitted before for any degree or examination in any other university, and that all the sources I have used or quoted have been indicated and acknowledged as complete references.

In this dissertation, unless otherwise stated or the context indicates differently, words importing the masculine gender include females and neuter, and vice versa. In addition, words in the singular number include the plural and vice versa.

This dissertation reflects the law in South Africa and in the foreign jurisdictions referred to as at 18 June 2024.

Full names: Marlin Lowell Fransman Submission Date: 18 June 2024

Signature:

UNIVERSITY of the
WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

ACKNOWLEDGEMENTS

While a study at this level is largely possible through a concerted effort by the candidate, there is a tribute to be paid to certain people without whom the completion of the dissertation would have been impossible.

My sincere gratitude is extended to my supervisors, Prof Fareed Moosa and Prof Vivienne Lawack, for their professional guidance, clarity of insights, patience and support.

I am also grateful to the organisers of the doctoral colloquium, and to Extra-ordinary Professor (Judge) Dennis Davis for his critical and constructive feedback.

I also wish to thank the Fintech Group for their input over the last couple of years.

I extend my deepest gratitude to Tracey-Lee Cloete for her invaluable feedback and comments on various draft chapters, and to Roxzan Fransman for her invaluable assistance in obtaining some of the materials, particularly those related to privacy, for the research.

Lastly, my utmost appreciation to my wife, Janine, for her unwavering support, patience and understanding throughout this study. I cannot thank her enough. Also, to my children Haidyn and Adam for their love, as well as my family, friends and colleagues for their encouragement and support.

UNIVERSITY of the
WESTERN CAPE

Hebrews 10:36

You need to persevere so that when you have done the will of God, you will receive what he has promised.

https://uwcscholar.uwc.ac.za/home

ABSTRACT

Technological advancements and the increasing speed of communication have given rise to the development of new products and business models. Personal information is a central element of these novel business models. Data subjects can exchange their personal information for goods and services, and businesses generate revenue by monetising such information. While the nexus between technology and personal information has long been recognised, personal information is traditionally seen as an integral aspect of privacy and is most often discussed in the context of privacy and data protection. In light of the commodification of personal information and the recognition of its economic value, it has become necessary to question whether personal information can be understood from a different legal perspective, namely, as property rights (or property interests).

This dissertation analyses the data protection regulatory framework in South Africa. The dissertation finds that South African data protection legislation affords data subjects a high level of protection that is comparable to that of the European Union. However, South African legislation does not address or recognise the commodification of personal information. Similarly, the South African Constitution, 1996 does not provide much guidance on this aspect. However, due to the transformative nature and effect of the Constitution, it allows for an interpretation of laws that reflects a changing legal landscape and changed mindset.

In this dissertation, an examination of the United States and the European Union reveals that, despite their differing approaches to data protection, the flow of personal information is an important enabler for economic development and creating value. The dissertation finds that data protection mechanisms in both jurisdictions seek to facilitate the flow of personal information and therefore promote the increasing commodification of personal information and its status as an asset.

It is concluded in this dissertation that because of contemporary data practices, personal information, under certain identified conditions, exhibits property-like characteristics and ought, it is submitted, to be eligible for protection as property under s 25 of the South African Constitution. Based on this and other conclusions, recommendations for a new legislative framework that supplements the current data protection framework, which is responsive to the commodification of personal information, are made.

https://uwcscholar.uwc.ac.za/home

KEYWORDS / TERMS

In this dissertation, the following keys words and/or terms are used:

Big data technologies

Commodification of personal information

Constitutional property

Data protection

Data-driven innovation

Intangibles

Medium of exchange

Personal data marketplace

Personal information

Privacy

https://uwcscholar.uwc.ac.za/home

ABBREVIATIONS

(i) General

ACM	Association for Computing Machinery
BEREC	Body of European Regulators for Electronic Communications
CC	Constitutional Court
CCPA	California Consumer Protection Act
CFR	Code of Federal Regulations
Constitution	Constitution of the Republic of South Africa, 1996
Convention 108	Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data
CJEU	Court of Justice of the European Union
Data Protection Directive	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data 1995 Official Journal L 281/31
DSM	Digital Single Market
EC	European Commission
ECHR	European Convention on Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Network and Information Security
EU	European Union
EUCFR	Charter of Fundamental Rights of the European Union
FIPs	Fair Information Practices
FIPPs	Fair Information Practice Principles
FTC	Federal Trade Commission
GDP	Gross Domestic Product

https://uwcscholar.uwc.ac.za/home

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 (General Data Protection Regulation), OJ 2016 L 119/1 (2016) repealing Directive 95/46/EC (Data Protection Directive)
GG	Government Gazette
GLBA	Gramm-Leach-Bliley Act
GN	Government Notice
GPS	Global Positioning System
HEW	United States Department of Health Education and Welfare
HIPAA	Health Insurance Portability and Accountability Act
IoT	Internet of Things
Lisbon Treaty	Treaty of Lisbon
KDD	Knowledge Discovery in Databases
Malabo Convention	African Union Convention on Cyber Security and Personal Data Protection
Mobile Apps	Mobile Software Applications
NCA	National Credit Act 34 of 2005
OECD	Organisation for Economic Co-operation and Development
PDA	Personal Digital Assistant
PETs	Privacy Enhancing Technologies
POPIA	Protection of Personal Information Act 4 of 2013
SALRC	South African Law Reform Commission
TFEU	Consolidated Version of the Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights
UCLA	University of California Los Angeles

UNIVERSITY of the WESTERN CAPE
https://uwcscholar.uwc.ac.za/home

URL	Uniform Resource Locator
US	United States of America
VC	Virtual Currency
VoIP	Voice Over Internet Protocol
WP29	The Working Party on the Protection of Individuals with regard to the Processing of Personal Data

(ii) Publications

IEEE	Institute of Electrical and Electronics Engineers
JOL	Judgments OnLine
PELJ	Potchefstroom Electronic Law Journal
SALJ	South African Law Journal
SAMLJ	South African Mercantile Law Journal
SAJEMS	South African Journal of Economic and Management Sciences
SMU	Southern Methodist University
THRHR	Tydskrif vir Hedendaagse Romeins-Hollandse Reg
TSAR	Tydskrif vir die Suid-Afrikaanse Reg

(iii) Referencing

art	article
fn	footnote
para	paragraph
s	section
subsec	subsection

https://uwcscholar.uwc.ac.za/home

CHAPTER ONE: INTRODUCTION AND RATIONALE FOR THE STUDY

1.1 BACKGROUND 11

1.2 PROBLEM STATEMENT AND RESEARCH QUESTIONS 14

1.3 RESEARCH OBJECTIVES 17

1.4 SIGNIFICANCE OF THE RESEARCH AND LITERATURE REVIEW 18

1.5 KEY TERMINOLOGY 22

1.5.1 Data-driven economy 22

1.5.2 Data protection 22

1.5.3 Data 23

1.5.4 Terms of art 23

1.5.4.1 Personal information 23

1.5.4.2 Data subject 24

1.5.4.3 Responsible party 24

1.6 RESEARCH METHODOLOGY 25

1.7 DELINEATION 26

1.8 OUTLINE OF ENSUING CHAPTERS 27

UNIVERSITY of the WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

1.1 BACKGROUND

The processing of personal information presents new opportunities for economic and societal value creation.[1] The Internet and advances in digital technology in the form of computers, laptops, smartphones, and tablets have facilitated and enabled, at relatively low costs, the collection, storage and processing of large quantities of personal information or data that have given rise to the so-called 'personal information economy'.[2] This economy is characterised by the use of information and technologies to drive economic activity.[3]

Companies, such as Facebook, Amazon, Microsoft, Apple, and Google, have recognised the value of personal information and have centred their respective business models around collecting and analysing it.[4] AT&T in the US is considering reducing telephone subscriptions for US customers who consent to targeted advertising.[5] In 2017, the Economist published an article proclaiming that the world's most valuable resource is no longer oil but rather data.[6] Significantly, Van Lieshout opines that such a comparison envisions personal information as being both a product in itself and a resource to drive economic activity.[7] Not surprisingly, technology and internet companies providing digital data products and services feature more prominently among the world's most valuable firms as opposed to oil and energy corporations.[8] Technology and the advanced analytical techniques that collect and analyse 'big data'[9] have

[1] World Economic Forum *Personal information: The Emergence of a New Asset Class* (2011) 5.

[2] Schwartz P 'Property, privacy and personal information' (2004) 117 *Harvard Law Review* 2055 2056–57.

[3] The 'data economy' refers to the increasing availability of data and the exploitation of such data to create business and revenue-generating opportunities. See BEREC *Report on the Data Economy* (2019) 106–7 available at *https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8599–berec–report–on–the–data–economy* (accessed 13 March 2020).

[4] Hoofnagle C & Whittington J 'Free: Accounting for the costs of the Internet's most popular price' (2013) 61 *UCLA Law Review* 606 628.

[5] Dang S et al 'Exclusive: AT&T considers cellphone plans subsidized by ads' *Reuters* 16 September 2020 available at *https://www.reuters.com/article/us–at–t–ceo–interview–exclusive/exclusive–att–considers–cellphone–plans–subsidized–by–ads–idUSKBN2663HK* (accessed 14 March 2023).

[6] The Economist 'The world's most valuable resource is no longer oil, but data' 6 May 2017 available at *https://www.economist.com/leaders/2017/05/06/the–worlds–most–valuable–resource–is–no–longer–oil–but–data* (accessed 6 June 2019). For an opposing view, see Marr B 'Here's why data is not the new oil' 6 June 2019 available at *https://www.forbes.com/sites/bernardmarr/2018/03/05/heres–why–data–is–not–the–new–oil/#7650084f3aa9* (accessed 6 June 2019). Marr argues that data, although inherently valuable, requires processing, just like oil requires refining before its true value can be unlocked.

[7] Van Lieshout M 'The value of personal information' in D Aspinall et al (eds) *Privacy and Identity* vol 457 (2014) 27.

[8] FXSSI 'Most valuable companies in the world – 2022' 27 July 2022 available at *https://fxssi.com/top–10–most–valuable–companies–in–the–world* (accessed 7 November 2022).

[9] De Mauro A, Greco M & Grimaldi M *What is big data? A consensual definition and a review of key research topics* (2015) 103. The authors define big data as 'information assets characterized by such a High Volume, Velocity and Variety to require specific Technology and Analytical Methods for its transformation into Value'.

https://uwcscholar.uwc.ac.za/home

allowed seemingly meaningless pieces of information to be organised in such a manner that they may be commercialised. Big data processing reflects the ability to collect, aggregate, and process increasing volumes, velocity, and variety of data from a number of technological sources.[10] This enables companies to compile customer profiles to increase both market intelligence and revenue flows; they do this through personalising the promotion of goods and services or tailoring advertisements for individual consumers based on personal information or past transactional activities.[11] Moreover, the data collected for economic purposes can also be subsequently sold and used in other situations, such as political manipulation or surveillance, leading to a continuous exchange between contexts where they are not only exploited for their economic worth but also treated as generic commodities.[12]

The relevance of personal information also extends to the public sector and plays an important role in improving public service efficiency and delivery.[13] On this point, the Organisation for Economic Co-operation and Development (OECD) states that the public sphere is a data-intensive sector that employs data analytics to develop products and services that drive growth and employment.[14] Therefore, personal information is understandably viewed as a valuable commodity.[15]

Big data technologies and data-driven innovation have given rise to new business models.[16] First, these business models have resulted in personal information being increasingly regarded as a tradeable asset and used as counter-performance.[17] For instance, consumers can acquire digital goods and services by simply exchanging or sharing their personal information without

[10] For examples of sources of big data, see White House *Big Data: Seizing Opportunities, Preserving Values* (2014) 5. Burns Y & Burger-Smidt A *Protection of Personal Information: Law and Practice* 2 ed (2023) 132 state that such processing uncovers patterns, trends and associations in large amounts of data.

[11] Schwartz P (2004) 2070.

[12] de Hingh A 'Some reflections on dignity as an alternative legal concept in data protection regulation' (2018) 19 *German Law Journal* 1269 1271.

[13] Van Lieshout M (2014) 28.

[14] OECD *Data-Driven Innovation: Big Data for Growth and Well-Being* (2015) 404 available at *https://doi.org/10.1787/9789264229358–en* (accessed 9 November 2022).

[15] Bottis M & Bouchagiar G 'Personal information v. Big data: Challenges of commodification of personal information' (2018) 8 *Open Journal of Philosophy* 206; Allotey A *Data Protection and Transborder Data Flows: Implications for Nigeria's Integration into the Global Network Economy* (unpublished LLD thesis, University of South Africa, 2014) 7.

[16] OECD *Data-Driven Innovation* (2015) 76. The diversity of revenue models includes advertisement-based models where services are provided for free or with a discount in exchange for viewing advertisements; the sale of sensor-equipped smart devices that generate data or the sale of digital content; and freemium models that comprise a free product with advertisements or limited functionality whereas the premium version is advertisement-free.

[17] Durovic M & Montanaro M 'Data protection and data commerce: Friends or foes?' (2021) 17 *European Review of Contract Law* 1 2.

https://uwcscholar.uwc.ac.za/home

the need for monetary payments. An exchange of personal information typically occurs (1) when a consumer submits personal information to sign up for free services (such as social media, YouTube and webmail) or digital services (such as Netflix for a limited trial period); (2) when a consumer downloads a free version of software that offers limited features but which offers full functionality if the entire purchase price is paid; or (3) when games or apps are downloaded for free from a digital store such as Google Play.[18] In return for the 'free' goods and services offered, the provider monetises the personal information that it collects.[19]

While the preceding paragraph may create the impression that a consumer acquires the digital goods or services for free because there is no monetary cost, such a consumer is actually offering value by sharing or making his personal information available in exchange for these goods and services. Personal information has, therefore, been described as a new kind of currency for the digital world.[20] In this regard, Nieman explains: 'Even time and personal information, when bartered to receive something in return, can be seen as VCs.'[21] The South African Reserve Bank defines a VC as 'a digital representation of value that can be digitally traded and functions as a medium of exchange, a unit of account and/or a store of value, but does not have legal tender status'.[22] This suggests that personal information has an inherent economic and commercial value.

Secondly, the economic exploitation of personal information resulting from these new business practices raises specific concerns. Challenges relating to the processing of personal information are typically characterised as matters of privacy. These challenges may include privacy harms, profiling, behavioural advertising and discrimination.[23] To safeguard people from the risks posed by the processing of personal information, it was necessary to introduce data protection regulations.[24]

---

[18] Additional content or game add-ons typically require monetary in-app purchases.

[19] Efroni Z 'Gaps and opportunities: The rudimentary protection for "data-paying consumers" under new EU consumer protection law' (2020) 57 *Common Market Law Review* 799 799.

[20] World Economic Forum (2011) 5; Eggers W, Hamill R & Ali A 'Data as the new currency: Government's role in facilitating the exchange' (2013) 13 *Deloitte Review* 18 19.

[21] Nieman A 'A few South African cents' worth on bitcoin' (2015) 18 *PELJ* 1979 1981.

[22] South African Reserve Bank 'Position paper on virtual currencies position paper' available at *https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014* (accessed 22 August 2019).

[23] Durovic M & Montanaro M (2021) 3. See 2.2.3 for a discussion on the privacy challenges.

[24] Roos A 'Core principles of data protection law' (2006) 39 *The Comparative and International Law Journal of Southern Africa* 102 105.

https://uwcscholar.uwc.ac.za/home

1.2 PROBLEM STATEMENT AND RESEARCH QUESTIONS

The legal problem is twofold. First, while technological innovation has facilitated trade by providing faster and easier ways to communicate and access a range of market opportunities, goods and services, it also poses significant regulatory challenges.[25] The capacity of databases to store and process increasing volumes of personal information has highlighted the need to ensure that privacy concerns, as a barrier to trade, are minimised, hence the enactment of data protection rules.[26] These rules have largely been developed in response to advances in technology. The objectives of these rules are to foster privacy by affording the data subject a measure of control over the way others process personal information while ensuring a free flow of information.[27]

In South Africa, the Protection of Personal Information Act (POPIA) was promulgated on 19 November 2013.[28] The basis for such protection is to safeguard a person's constitutional right to privacy, which is an important aspect of personality.[29] Similarly, in the broader African context, the purpose of the Convention on Cyber Security and Personal information Protection (the Malabo Convention)[30] is to establish a framework for personal information protection that promotes individuals' right to privacy.[31] In this regard, Abdulrauf and Fombad state that the Malabo Convention demonstrates an unequivocal commitment to upholding and respecting human rights and fundamental freedoms.[32] Therefore, the legal protection provided is not based on the idea that individuals have property rights over their personal information but rather on

[25] Sorieul R, Clift J & Estrella-Faria J 'Establishing a legal framework for electronic commerce: The work of the United Nations Commission on International Trade Law (UNCITRAL)' (2001) 35 *The International Lawyer* 107 107. See also 3.1 below.

[26] SALRC *Project 124: Privacy and Data Protection Report* (2009) vi–vii.

[27] SALRC (2009) para 3.2.4. These dual objectives also underpin the European data protection framework. See 5.2 below.

[28] Act 4 of 2013. It was enacted in terms of GN 912 in GG 37067 of 26 November 2013. However, GN 10173 in GG 37544 of 11 April 2014 proclaimed only certain provisions relating to the definitions and Information Regulator to be effective. The President of South Africa issued Proc R21 in GG 43461 of 22 June 2020 for the remainder of the operative provisions to come into force from 1 July 2020.

[29] Batchelor B & Wazvaremhaka T 'Balancing financial inclusion and data protection in South Africa: Black Sash Trust v Minister of Social Development' (2019) 136 *SALJ* 112 120–21.

[30] African Union Convention on Cyber Security and Personal information Protection EX.CL/ 8 4 6 (XXV) (2014).

[31] Article 8(1), Malabo Convention.

[32] Abdulrauf L & Fombad C 'The African Union's data protection Convention 2014: A possible cause for celebration of human rights in Africa?' (2016) 8 *Journal of Media Law* 67 76.

https://uwcscholar.uwc.ac.za/home

the aim of regulating the processing of personal information in a manner that fosters dignity and autonomy.[33]

Despite the human rights aspirations of these data protection frameworks, some scholars like Victor argue, with merit, that these rights-based frameworks employ property-like features that lend themselves to a property-based perspective.[34] Such a property-based conception becomes problematic when the purpose of the data protection instrument is to regulate the processing of personal information in a manner that recognises and promotes human rights rather than treating it as a commodity that is capable of exchanging hands.

Secondly, personality rights are non-patrimonial in nature, cannot exist independently of a person and are inextricably linked with such a person's personality.[35] Privacy, as an aspect of personality rights, cannot be relinquished, alienated or transferred to others.[36] Based on such reasoning, it could be argued that personal information cannot be sold, exchanged or transferred.

However, data-driven innovation has given rise to new business models not anticipated by data protection rules, such as personal information being treated as a commodity and used as a medium of exchange to acquire digital goods and services. When personal information is used in this manner, the information appears to be the object of the transaction. This seems to conflict with the notion that privacy and, by implication, personal information are inalienable. Such an exchange constitutes a commodification of privacy, particularly with regard to personal information. To commodify something means to turn it into an object for sale.[37] Schwartz describes commodified personal information as a discrete, tradeable bundle of information.[38] This is consistent with the view that personal information is an asset.[39]

[33] Roos A 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124 *SALJ* 400 402–3.

[34] Victor J 'The EU General Data Protection Regulation: Toward a property regime for protecting data privacy' (2013) 123 *The Yale Law Journal* 513 515.

[35] Neethling J 'Personality rights: Comparative overview' (2005) 38 *Comparative and International Law Journal of Southern Africa* 210 223; *Kumalo v Cycle Lab (Pty) Ltd* [2011] JOL 27372 (GSJ) para 32.

[36] Neethling J (2005) 223.

[37] Radzik L & Schmidtz D 'Contested commodities' (1997) 16 *Law and Philosophy* 603 603.

[38] Schwartz P (2004) 2069.

[39] de Stadler E & Esselaar P *A Guide to the Protection of Personal Information Act* (2015) para 1.3.1; Bottis M & Bouchagiar G 'Personal information v. Big data: Challenges of commodification of personal information' (2018) 8 *Open Journal of Philosophy* 206 206; Snail S & Papadopoulos S 'Privacy and data protection' in Papadopoulos S & Snail S (eds) *Cyberlaw@SA IV: the law of the Internet in South Africa* 4 ed (2022) 307-8.

https://uwcscholar.uwc.ac.za/home

This raises the question of whether personal information, when used as a medium of exchange, could qualify as a form of 'property'. Data protection entails protecting and regulating the processing of personal information of one person by a third party; in contrast, the use of personal information as a medium of exchange necessitates examining personal information as an object of property rights.

Extending property protection to personal information may be justified in certain circumstances because personal information is viewed as a tradeable commodity and an asset with economic value. By investigating whether personal information could qualify as 'property', recommendations can be made as to the circumstances under which personal information ought to be identified as a commodity and qualify for protection as property.

Against the background outlined above, this dissertation ventilates and postulates answers to the general research question whether personal information can be recognised and protected for purposes of the constitutional property clause and, if so, under what circumstances. In answering this general question, answers to the following consequential sub-questions are also explored:

Chapter two:

(i) What are the technological enablers of the personal information trade and the implications for the privacy of data subjects? This question delves into the commodification of personal information and the concerns resulting from this development in commerce within a technologically advanced arena.

Chapter three:

(ii) What entitlements do data subjects enjoy under the South African data protection law, and are such entitlements effective given the personal information trade? This question explores the conceptual framework underpinning the South African data protection law and assesses the effectiveness of data protection rights in the light of current data processing practices.

UNIVERSITY of the WESTERN CAPE
https://uwcscholar.uwc.ac.za/home

Chapter four:

(iii) To what extent, given the commodification of personal information, could a property regime serve to regulate the use of resources? This question investigates the dynamics driving the allocation of economic value from personal information.

Chapter five:

(iv) In view of the commodification of personal information, could personal information be propertised in any sense? This question delves into various legal frameworks regulating the processing of personal information and their role in shaping the propertisation of personal information.

Chapter six:

(v) To what extent, if any, may personal information be recognised as 'property' at common law? Moreover, could the property clause in s 25 of the Constitution accommodate modern-day interests, such as personal information? These questions explore the South African concept of property in the light of, among other things, prevailing data processing practices.

UNIVERSITY of the
WESTERN CAPE

1.3 RESEARCH OBJECTIVES

This dissertation aims to:

(i) critically discuss and evaluate the existing data protection framework in South Africa and determine whether such a data protection scheme could be viewed as promoting the propertisation of personal information;

(ii) determine whether it is possible to recognise personal information as an object of property rights;

(iii) determine whether recognition of property rights in personal information is compatible with a human rights-based approach to privacy; and

https://uwcscholar.uwc.ac.za/home

(iv) propose recommendations as to the circumstances under which personal information ought to be identified as a commodity and qualify for protection as constitutional property.

1.4 SIGNIFICANCE OF THE RESEARCH AND LITERATURE REVIEW

The advances in technology since the advent of South Africa's constitutional democracy in 1994 and the opportunities it presents for the development of new products and innovative business models have led (as discussed above) to personal information being treated as a valuable commodity. Its use as such is likely only to increase with the passage of time.

In accordance with the Constitution, South Africa subscribes to a human rights ethos based on the values of equality, dignity and freedom. Although the Bill of Rights entrenches the rights to privacy and to property, it does not expressly refer to, or expressly treat, 'personal information' (or data) as property or property interests. This is probably because the Bill was written at a time when trading in personal information was, largely, unknown. However, if the Constitution is to remain relevant in the lives of ordinary South Africans, then it must keep pace with changing times and societal needs. It is against this backdrop that the research questions formulated above are to be viewed. They pose novel questions in a South African legal cum constitutional setting.

UNIVERSITY of the
WESTERN CAPE

A literature review has revealed a dearth of scholarship on property rights in personal information in South Africa. Only one reported case briefly touches on property rights in personal information as a side aspect without offering a clear elucidation of the issue.[40] Personal information is most often discussed in the context of data protection. Burns and Burger-Smidt state in their most recent commentary on data protection published in 2023 that the protection and regulation of personal information in South Africa are encompassed within the sphere of the law of privacy.[41] This is so because the processing of personal information implicates aspects of dignity and autonomy. Despite Burns and Burger-Smidt recognising that personal information is used to create new products and services,[42] the authors do not explore personal information from a property standpoint.

[40] See *Discovery Ltd and Others v Liberty Group Ltd* 2020 (4) SA 160 (GJ).
[41] Burns Y & Burger-Smidt A (2023) 56.
[42] Burns Y & Burger-Smidt A (2023) 785–86.

https://uwcscholar.uwc.ac.za/home

A few other South African scholars have considered information-based, intangible interests from a property perspective. Thaldar et al examine the multidimensional legal nature of personal genomic sequence data.[43] Thaldar et al place significant emphasis on the common law ownership of such data, how ownership ought to be allocated and the effects of competing rights on ownership. Although Thaldar et al's article contributes to the understanding of whether derived data can be considered property, this dissertation explores the property question in relation to personal data exchanged by data subjects by focusing primarily on the protection of property as opposed to ownership.

Moosa argues that cryptocurrency, which implicates privacy interests because it is linked to digital wallets containing personal information, ought to be considered constitutional property for the purposes of s 25 of the Constitution.[44] The thrust of Moosa's argument rests on cryptocurrencies, which possess inherent property-like features, having a convertible value for tax administration purposes based on a contextual reading of the Constitution. While Moosa's article provides a useful contribution insofar as it relates to the interpretation of the Constitution for the inclusion of intangible interests hitherto not recognised as property, it does so in relation to an interest that, in commerce, may be more readily acceptable as a form of property.[45] This dissertation explores personal information as a distinct entity separate from other proprietary interests with which it may be associated.

Erlank examines the legal significance of intangible property in online environments, which he refers to as 'virtual property'.[46] Erlank states that virtual property meets all the required characteristics of a 'thing' and argues that since virtual property can be owned, acquired, used, possessed or disposed of, it ought to receive the same legal recognition as traditional forms of property.[47] Erlank accepts that certain things, like email and website addresses (URLs),[48] are property and does so on the basis that such things are inherently rivalrous, which means that no two people are likely to have the same information.[49] However, Erlank's discussion is not

[43] Thaldar D et al 'The multidimensional legal nature of personal genomic sequence data: A South African perspective' (2022) *Frontiers in Genetics* 1 1–11.

[44] Moosa F 'Is cryptocurrency "property" for tax administration purposes?' (2021) 33 *SAMLJ* 364 380–83.

[45] In a recent high court decision, bitcoin was recognised as property for insolvency purposes. See *Bester NO and Others v Mirror Trading International (Pty) Ltd t/a MTI (In Liquidation) and Others* 2024 (1) SA 112 (WCC) para 50.

[46] Erlank W 'Introduction to virtual property: Lex Virtualis Ipsa Loquitur' (2015) 18 *PELJ* 2525 2525–34.

[47] Erlank W 'Law and property in virtual worlds' in Barfield W & Blitz M (eds) *Research Handbook on the Law of Virtual and Augmented Reality* (2018) 636–57.

[48] A URL is an easily readable series of characters that directs a browser to a desired website on the Internet.

[49] Erlank W *Property in Virtual Worlds* (unpublished LLD thesis, University of Stellenbosch, 2012) 276–77.

https://uwcscholar.uwc.ac.za/home

framed through the lens of personal information. This dissertation explores property rights in personal information, which is generally non-rivalrous in nature as it is capable of being used by two or more parties simultaneously without being depleted.

Njotini supports the idea of property rights in information or data because of its importance to society.[50] Njotini challenges the embedded understanding of property as being corporeal in nature and advocates for the inclusion of incorporeals. The focus of his article concerns intangible interests such as computer data and not personal information as envisaged in a data protection context.[51] Njotini refers briefly to s 25 of the Constitution, however, the article lacks a critical analysis of the pertinent constitutional provisions. Njotini primarily focuses on the private law perspective of property throughout the discussion. This dissertation examines property rights under constitutional law, as opposed to only focusing on private law.

Kellerman identifies several unconventional immaterial interests that may or may not be protected under private law but which ought to be afforded protection under s 25 of the Constitution.[52] These unconventional immaterial interests all share property characteristics recognised under private law. This dissertation expands on Kellerman's work by focusing on personal information as a new unconventional immaterial interest that could potentially qualify for protection under s 25 of the Constitution.

Beyond South Africa, the propertisation of personal information has been debated extensively in the United States (US)[53] and the European Union (EU).[54] In the US, property rights in personal information aim to enhance data protection while still allowing for the transferability

[50] Njotini M 'Evaluating the position of information or data in the law of property' (2015) 26 *Stellenbosch Law Review* 220 220–39.

[51] Njotini M (2015) 221 seemingly rejects the proposition that personal information could qualify as a form of property.

[52] Kellerman M *The Constitutional Property Clause and Immaterial Property Interests* (unpublished LLD thesis, University of Stellenbosch, 2011) 49–108.

[53] Baron J 'Property as control: The case of information' (2012) 18 *Michigan Telecommunications and Technology Law Review* 367 369; Purtova N 'Property rights in personal data: Learning from the American Discourse' (2009) 25 *Computer Law and Security Review* 507 507; Schwartz P 'Property, privacy and personal information' (2004) 2057–58; Lemley M 'Private Property' (2000) 52 Stanford Law Review 1545 1546; Lessig L 'Privacy as property' (2002) 69 *Social Research* 247 247; Samuelson P 'Privacy as intellectual property?' (1999) 52 *Stanford Law Review* 1125 1127; Laudon K 'Markets and privacy' (1996) 39 *Communications of the ACM* 92 92.

[54] Janeček V 'Ownership of personal data in the Internet of Things' (2018) 34 *Computer Law & Security Review* 1039 1039–52; Lynskey O *The Foundations of EU Data Protection Law* (2015) 231–37; Victor J (2013) 515–16; Purtova N 'Property in personal data: A European perspective on instrumentalist theory of propertization' (2010) 2 *European Journal of Legal Studies* 193 195; Prins C 'Property and privacy: European perspectives and the commodification of our identity' in Guibault L & Hugenholtz P (eds) *The Future of the Public Domain* (2006) 224.

https://uwcscholar.uwc.ac.za/home

of personal information. The propertisation debate from an EU perspective explores the protective function of property as opposed to a tool that facilitates the exchange of personal data. The US and the EU do not legally recognise property rights in personal information, despite the substantial body of scholarly works that exist. None of the jurisdiction-specific literature delves into the meaning of property, to the extent that it relates to personal information, from a constitutional perspective.

Purtova observes that discussions about the economic value and ownership of personal information continue to remain an ongoing debate,[55] which is testament to the current relevance of the issues raised by the intersection of property and personal information. It appears, based on the literature survey, that this is the first study researching the propertisation of personal information in South Africa and Africa, more broadly. This dissertation potentially provides a valuable contribution to the academic literature, particularly because there is presently no comprehensive known dissertation which investigates the propertisation of personal information generally in a South African context. It is submitted that the research topic is relevant to other African countries grappling with similar issues relating to the commodification of personal information. In support of this claim, Mtweve contends that if Tanzania's constitution recognises personal data as an asset or property, it would protect the data ownership rights of individuals due to the increasing commercialisation of personal data and its treatment as an asset by technology companies.[56]

The question explored in this dissertation, namely, whether personal information constitutes constitutional property becomes more relevant given its commodification in everyday commerce coupled with the fact that the propertisation of personal information remains largely unexplored in the South African context. As a general hypothesis, there are no privacy or data protection laws in South Africa or the jurisdictions referred to above that equate personal information with property.

[55] Purtova N (2015) 85.

[56] Mtweve E 'Data as Property (Article 7)' (16 August 2022) available at *https://victoryattorneys.co.tz/data-as-property-article-7/* (accessed 22 December 2023).

https://uwcscholar.uwc.ac.za/home

1.5 KEY TERMINOLOGY

A number of key terms used throughout this dissertation need to be clarified. Some of these terms are explained below.

1.5.1 Data-driven economy

The data-driven economy or data economy refers to businesses that utilise data as their core activity.[57] No generally accepted definition of the data economy currently exists, but it involves reusing data and employing data analytics to create new business opportunities and foster new products and services.[58] The terms data-driven economy and data economy are used interchangeably in this dissertation.

1.5.2 Data protection

Data protection refers to the legal protection accorded to data subjects in relation to the collection, processing, storage, and deletion of their personal information by a third party.[59] Data protection involves the processing of personal information according to established and recognised principles.[60] The aim of data protection is to enable data subjects to have greater control over the processing of their personal information.[61] Therefore, the principles aim to ensure lawful processing rather than to prohibit any processing. The term 'data protection' is used as a term of convenience for describing the laws and principles that have been adopted to protect personal information in a variety of international, national and regional data protection frameworks.

[57] See fn 3 above.

[58] BEREC Report on the Data Economy (2019) 106.

[59] Roos A (2007) 402–3; Naude A & Papadopoulos S 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (1)' (2016) 79 *Journal of Contemporary Roman-Dutch Law* 51 52–3; Swales L 'The Protection of Personal Information Act 4 of 2013 in the context of health research: Enabler of privacy rights or roadblock?' (2022) 25 *PELJ* 1 6.

[60] Roos A (2006) 108–27.See for example section 4(1) of POPIA.

[61] Neethling J (2012) 244.

https://uwcscholar.uwc.ac.za/home

1.5.3 Data

Janeček distinguishes between the terms 'data' and 'information'.[62] Data is generally interpreted in relation to information as raw facts or figures, whereas information consists of processed data that has meaning.[63] Therefore, data can be understood as the source of information.[64] Various South African scholars are, however, of the opinion that, in the literature on data protection, both terms bear similar meanings. Roos,[65] Naude and Papadopoulos,[66] and Burns and Burger-Smidt consider the terms interchangeable.[67] Roos states it is overly pedantic to maintain such a difference in data protection literature.[68] For example, in the General Data Protection Regulation (GDPR),[69] recital 6 and art 4(1) use the terms 'personal data' and 'personal information' interchangeably. Therefore, the terms 'data' and 'information' are also used interchangeably in this dissertation.

1.5.4 Terms of art

For the sake of consistency, this dissertation adopts the terms used in POPIA. Unless otherwise specified, such terms encompass equivalent terms and have similar meanings when used in relation to the data protection legislation of other jurisdictions. Quotes from scholarly literature are based on the author's terms and, unless otherwise indicated, should be understood to include equivalent POPIA terms.

1.5.4.1 Personal information

This dissertation uses the term 'personal information' to indicate that the information falls within the protective scope of the data protection legislation selected for this dissertation. For

---

[62] Janeček V 'Ownership of personal data in the internet of things' (2018) 34 *Computer Law & Security Review* 1039 1042.

[63] Stepanov I 'Introducing a property right over data in the EU: The data producer's right – an evaluation' (2019) *International Review of Law, Computers & Technology* 1 3.

[64] Stepanov I (2019) 3.

[65] Roos A *The law of data (privacy) protection: A comparative and theoretical study* (unpublished LLD thesis, University of South Africa, 2003) 18.

[66] Naude A & Papadopoulos S (2016) 60.

[67] Burns Y & Burger-Smidt A (2023) 2.

[68] Roos A *The law of data (privacy) protection: A comparative and theoretical study* (2003) 18.

[69] 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, OJ 2016 L 119/1.

https://uwcscholar.uwc.ac.za/home

the reasons mentioned above, the term 'personal information' may be used interchangeably with 'personal data'.[70] Personal information is broadly defined as information relating to identifiable, living, natural persons.[71] Personal information is capable of differentiating individuals from each other.

1.5.4.2 Data subject

A data subject is any person to whom the personal information relates.[72] A data subject can be identified, directly or indirectly, by reference to any information that relates to physical, physiological, mental, economic, cultural or social identity.[73] In this dissertation, unless the context indicates otherwise, the term 'data subject' has a meaning similar to the terms 'individual' or 'consumer' insofar as it relates to the processing of personal information. Depending on the jurisdiction under discussion, this dissertation refers to the more commonly used term. Nonetheless, the terms are interchangeable and are used as such.

UNIVERSITY of the
WESTERN CAPE

1.5.4.3 Responsible party

Under POPIA, a 'responsible party' is a person, either public or private, who alone or in conjunction with others determines the purpose of and means for processing personal information.[74] POPIA distinguishes between a 'responsible party' and the 'operator'. The operator is responsible for processing the personal information on behalf of the responsible party without being directly controlled by them.[75] This envisages a scenario where businesses outsource the processing of personal information to others. The GDPR uses the terms 'data controller'[76] and the 'data processor',[77] which are synonymous with 'responsible party' and 'operator' respectively. However, for the purposes of this dissertation, it is not strictly necessary to maintain a distinction between the roles of the persons involved in processing

[70] See 1.5.3 above.
[71] Section 1, POPIA. In contrast to the data protection instruments of the EU and US, personal information as defined in POPIA also applies to juristic persons.
[72] Section 1, POPIA.
[73] Section 1, POPIA; Art 4(1), GDPR.
[74] Section 1, POPIA.
[75] Section 1, POPIA.
[76] Article 4(7), GDPR.
[77] Article 4(8), GDPR.

https://uwcscholar.uwc.ac.za/home

personal information of data subjects. Therefore, for sake of convenience and unless the context indicates otherwise, persons who process personal information are referred to either as 'responsible parties', 'data processors', 'businesses', 'organisations' or 'companies'. Consequently, these terms will be used interchangeably.

1.6 RESEARCH METHODOLOGY

The research was conducted using published materials. This dissertation is not an empirical dissertation; instead, the dissertation makes use of a desktop methodology. This involves conducting a critical review and analysis of international, regional and national instruments, and case law relating to the right to data protection. The key secondary sources relied on include books, journals, newspaper and online articles, research reports, and theses.

Since data protection is regulated by means of legislation in all the jurisdictions being considered, a major part of this dissertation is devoted to a discussion of the applicable data protection frameworks. This discussion is grounded in the constitutional protection of the right to privacy and related rights, which underpin data protection laws in the United States (US), European Union (EU) and South Africa.

The aforementioned discussion provides the basis for the discussion of property rights in personal information. Given that personal information has economic value and is treated similarly to a commodity, the evolution of property law principles is also examined. In this regard, unconventional and traditional immaterial property interests are investigated to determine whether personal information could be relevant to the practice of the law of property.

A comparative method is employed to examine the legal position in a selection of foreign legal systems, namely the US and the EU. However, this dissertation does not embody a fully-fledged comparative analysis dealing with all the intricacies of these legal systems. Rather, the use of legal comparative methodology is adapted and limited to what is, in my opinion, necessary for the purposes of answering the research questions, with reference also to the propertisation of personal information in various other jurisdictions. The experiences in those jurisdictions in addition to practical considerations such as the accessibility and availability of primary and secondary source material that can serve as practical comparative sources informed the selection of the abovementioned jurisdictions. The reason for selecting the US

https://uwcscholar.uwc.ac.za/home

and EU draws on their historical and ongoing influence on South African privacy jurisprudence.

The US is chosen because it was US scholars who first proposed that personal information be recognised as property as a result of being treated as a commodity. The US position is characterised by an individual being viewed as a participant in the marketplace and by the fact that such an individual is a trader of a commodity, namely personal information.[78] Due to the shortcomings of the US data protection regime in providing individuals with adequate control over their personal information, the function of property rights would be to compensate for these shortcomings and increase data protection. Moreover, the US has the world's largest economy and is home to several major technology businesses that focus on processing personal data. As the US does not have an omnibus privacy statute at the federal level that is applicable to both the public and the private sectors, only relevant statutes at the federal and state levels have been selected for discussion.

The EU is selected based on its human rights-oriented approach to privacy and data protection. The EU is chosen in part because it has recently undergone a process of modernisation and harmonisation to support the concept of a single digital market across its member states and to ensure harmonised legal rules governing the flow of personal information. The GDPR is selected for discussion because it introduces new norms and best practices for data protection laws globally.[79] South African data protection legislation is modelled on the European approach to data protection. Given that EU data protection jurisprudence is by far the more matured, South African courts are likely to seek guidance in their developments. Reference is also be made to other relevant legal frameworks at an EU level that have been adopted for the purposes of regulating personal information transfers in more commercial settings.

1.7 DELINEATION

The scope of this dissertation will cover areas relating to the law of privacy, data protection and property. However, an in-depth discussion of the law of privacy and all the substantive provisions of data protection legislation is beyond the scope of this dissertation. As this

[78] Schwartz P & Peifer K (2017) 115 121.

[79] Buttarelli G 'The EU GDPR as a clarion call for a new global digital gold standard' (2016) 6 *International Data Privacy Law* 77 77.

https://uwcscholar.uwc.ac.za/home

dissertation is concerned with the interface between personal information and property, only those aspects of data protection deemed relevant to this dissertation have been selected.

Moreover, the dissertation is limited to a discussion of the CC's approach to the nature of 'property' for the purposes of s 25 of the Constitution. Accordingly, only those CC decisions which are deemed relevant in this context will be considered to determine the basis for the inclusion of new intangible, unconventional property interests into the constitutional conception of 'property'. Except for a brief statement on deprivation, issues dealing with deprivation or expropriation are not discussed - these issues are irrelevant for achieving the stated aims of this dissertation.

1.8 OUTLINE OF ENSUING CHAPTERS

Chapter two considers technological developments that are prevalent in the data-driven economy which have given rise to concerns pertaining to personal data processing. The chapter examines selected technologies and their impact on the processing of personal information. These processing activities have led to privacy and data protection concerns. To comprehend these problems more effectively, the model developed by Tal Zarsky is utilised to analyse the three stages of personal information flow: collection, analysis and data application.

Chapter three assesses the conceptual framework underpinning the South African privacy and data protection regime. This analysis focuses attention on the rights and remedies afforded to individuals by data protection legislation and on whether it can adequately deal with (i) the privacy concerns of individuals in the data economy and (ii) the manner in which personal information is being used as a medium of exchange. This chapter discusses protecting personal information as part of one's identity, whereas the next chapters delve into personal information as a commodity.

Chapter four explores the idea of property rights in personal information in the US, where it first originated. The chapter starts by analysing the legal identity of the US, specifically as it relates to the treatment of personal information in a market-driven discourse and the way such attitudes are generally reflected in the US approach to data protection. Data protection or information privacy, as it is more commonly referred to in the US, has its roots in the law of tort and the constitutional law. However, the law of tort and the constitutional law of privacy have proved ineffective in providing safeguards to protect privacy from the increasing use of computer technology, and, more recently, big data technologies. Consequently, this has

https://uwcscholar.uwc.ac.za/home

resulted in a muddled, inconsistent patchwork of torts, constitutional and statutory laws, leaving significant gaps in data protection. Property rights in personal information are presented as an alternative solution to fill in the gaps.

Chapter five explores the idea of property rights in personal information from a EU perspective. The discussion starts by analysing the EU's approach to data protection as a fundamental right and its treatment of personal information in an environment that is being increasingly challenged by personal data-driven innovation. In the EU, fundamental rights underpin privacy and data protection. As such, an individual's right to the protection of personal information is anchored in the interests of dignity and personality. From a EU perspective, it is argued that personal information is inextricably linked to the personality of the individual and is therefore non-commodifiable. Despite the adoption of such a position by the EU, it is demonstrated that EU data protection legislation facilitates the exchange of personal information by mimicking property-like characteristics. Moreover, technological advancements have made possible new business models based on personal information; consequently, new legislative mechanisms have been promulgated to regulate these new business practices. As personal information becomes a central feature of commercial exchanges and given the increasing importance of personal information in an economic context, the chapter investigates whether the treatment of personal information as something that is non-commodifiable is still relevant given current data practices.

UNIVERSITY of the
WESTERN CAPE

Chapter six deals with the recognition and possible protection of personal information as constitutional property. This chapter discusses the meaning of 'property' in private law and constitutional law, respectively. Accepting that personal information does have economic value and shares similar characteristics with property, the chapter discusses the possibility that it could be included under the constitutional property concept.

Chapter seven provides the conclusions of the dissertation and various recommendations.

https://uwcscholar.uwc.ac.za/home

CHAPTER TWO: TECHNOLOGICAL DEVELOPMENTS AND THE PRIVACY CHALLENGES POSED BY NEW TECHNOLOGIES

2.1 INTRODUCTION 30

2.2 DEVELOPMENTS GIVING RISE TO PERSONAL DATA CONCERNS 30

2.2.1 Convergence of technology and personal information 30

2.2.2 The Internet 32

2.2.3 Cloud computing 33

2.2.4 Smart devices 35

2.2.5 Internet of things (IoT) 38

2.3 PRIVACY CHALLENGES 40

2.3.1 The challenge of big data for personal Information 41

2.3.2 Collection: secrecy and consent 42

2.3.3 Analysis of personal data: predictive analysis, profiling, and power asymmetry 45

2.3.4 Implementation 48

2.3.4.1 Profiling 48

2.3.4.2 Re-identification 51

2.3.4.3 Behavioural targeting 54

2.3.4.4 Discrimination 55

2.3.4.5 Re-use and secondary uses of personal information 57

2.4 CONCLUSION 59

UNIVERSITY of the WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

2.1 INTRODUCTION

As mentioned in chapter one, modern technology and on-going technological developments give rise to real concerns pertaining to personal data processing, particularly their impact on privacy and data protection.[80] This is so because technology has facilitated the interconnectedness of everyday objects, allowing for the ubiquitous monitoring of data subjects' lives and the unprecedented collecting and processing of personal information. Big data technologies offer potential benefits to various industries by employing analytical techniques to find value in the vast quantities of data being collected, processed and aggregated, which can ultimately improve and benefit businesses and society. As such, personal data takes on a distinct character beyond being just a feature of an individual's personality—something that has not been explored in any great detail in the South African context. This claim will be explored in further detail in the subsequent chapters.

Despite the new opportunities that big data technologies offer, they also present significant challenges to privacy. The interconnectedness occasioned by big data technologies results in a borderless flow of personal information. Data may be collected from various sources, analysed, and used without the knowledge of data subjects. First, this chapter discusses various technologies that play a prominent role in the big data era. Secondly, the application of the big data technologies presents several privacy risks and challenges. These privacy challenges are numerous and are discussed in a structured manner using the personal data flow model proposed by Tal Zarsky.[81]

UNIVERSITY of the
WESTERN CAPE

2.2 DEVELOPMENTS GIVING RISE TO PERSONAL DATA CONCERNS

2.2.1 Convergence of technology and personal information

> 'Privacy is one of the biggest problems in this new electronic age. At the heart of the Internet culture is a force that wants to find out everything about you. And once it has found out everything about you and two hundred million others, that's

[80] See 1.1 above.
[81] See 2.3 below.

https://uwcscholar.uwc.ac.za/home

> a very valuable asset, and individuals will be tempted to trade and do commerce with that asset. …'[82]

The quote above aptly describes the reality that individuals must contend with daily. The ubiquitous monitoring of individuals' behaviour and habits provides new business opportunities for companies to monetise personal data. Grove anticipates the typical privacy challenges but, importantly, also identifies the issue of commodification of personal data that extends beyond privacy. The influence of technology is apparent in helping shape these legal issues.

Discussions about privacy and personal information have evolved with and in response to the development of technology.[83] The unprecedented increase in data storage, processing, and transmission capacities, miniaturisation,[84] interoperability,[85] ubiquity,[86] and convergence, as discussed below, occasioned by technological developments that are typical of the big data era, presents a number of challenges for privacy and data protection.[87] New technologies undermine privacy by facilitating the collection, storage, and processing of personal data by both the government and the private sector.[88] Large volumes of data are collected from multiple sources and subjected to aggregation and analytical techniques to generate new insights that would not have been possible using only the original or individual pieces of information.[89] The trend of collecting and combining information from different, independent sources or technologies that integrate to form a new outcome is referred to as 'technological convergence'.[90] Technological

[82] Sager M 'Andy Grove: What I've learned' *Esquire* 2007 available at https://www.esquire.com/features/what–ive–learned/learned–andy–grove–0500 (accessed 9 July 2020).

[83] Van den Hoven J et al 'Privacy and information technology' in Zalta E (ed) *The Stanford Encyclopedia of Philosophy* (2020) para 1 available at https://plato.stanford.edu/archives/sum2020/entries/it–privacy/ (accessed 9 July 2020).

[84] Miniaturisation represents the physical shrinking in size of electronic components to enable the development of new technologies. See Purtova N *Property Rights in Personal Data* (published PhD thesis, Tilburg University, 2011) 18.

[85] According to the EC *Big Data Interoperability Analysis* (2018) 2–3, interoperability can have different meanings depending on the context that is being looked at. At a semantic level, big data interoperability revolves around the ability of two systems to communicate and exchange data.

[86] Ubiquity refers to the trend of embedding sensors in everyday objects so that they are capable of communicating and transmitting data at any time and in any place. See Rouse M 'Ubiquitous Computing' *Technopedia* 18 March 2014) available at https://www.techopedia.com/definition/22702/ubiquitous–computing (accessed 12 April 2023).

[87] Gutwirth S et al (eds) *Computers, privacy and data protection: An element of choice* (2011) v.

[88] Friedewald M & Pohoryles R 'Technology and privacy' (2013) 26 *Innovation: The European Journal of Social Science Research* 1 1.

[89] Altman M et al 'Practical approaches to big data privacy over time' 8 *International Data Privacy Law* 29 29–30.

[90] Congressional Research Service *Technological convergence: Regulatory, digital privacy, and data security issues* (2019) 1.

https://uwcscholar.uwc.ac.za/home

convergence devices comprise of 'smart' or 'internet of things'[91] devices that are connected to a network and each other and have the ability to collect, use, and share data autonomously.[92] Such convergence has contributed significantly to the commodification of personal data, which raises new questions about how personal data ought to be treated in the data economy and whether the consideration of alternative regulatory frameworks are warranted to adequately deal with the commodification of personal data.

2.2.2 The Internet

The Internet began in 1969, when the US Department of Defense created a decentralised network of computers to reduce the risk of information or communication being lost in the event of a nuclear attack.[93] The Internet is described as an interconnected system of networks that makes it possible for computers to communicate with each other using a common set of standards or protocols.[94] The Internet's use was extended into a secret, highly organised communication system between the military, defence contractors, and university researchers engaged in classified military research; subsequently, the Internet increasingly became a tool used by university researchers for personal communication and sharing of non-classified research.[95]

The Internet has since developed beyond its early military research roots to support and facilitate commercial activity on a large scale. Leiner et al observe that, whereas initial commercialisation efforts primarily consisted of vendors offering basic Internet access and connectivity services, the Internet, as a global information infrastructure, is now used to support other commercial services, such as the provision of sophisticated information-based products and services.[96] These services include electronic mail and online messaging systems; file

[91] Baker E 'Trustless property systems and anarchy: How trustless transfer technology will shape the future of property exchange' (2015) 45 *Southwestern Law Review* 351 368 states that: 'The "Internet of Things" is a buzz phrase in the techy community that refers to the recent boom in connected devices and chattels.'

[92] Congressional Research Service (2019) 4–5.

[93] Van der Merwe D et al *Information and communications technology law* 2 ed (2016) 14.

[94] For a definition of the Internet see s 1 of the Electronic Communications and Transactions Act 25 of 2002. See also Pistorius T 'Formation of internet contracts: An analysis of the contractual and security issues' (1999) 11 *SAMLJ* 282 282.

[95] Hofman J et al *Cyberlaw A guide for South Africans doing business online* (1999) 11; Lawack V *Aspects of internet payment instruments* (unpublished LLD thesis, University of South Africa, 2001) 18–24.

[96] Leiner B et al 'A brief history of the internet' (2009) *ACM SIGCOMM Computer Communication Review* 22 30.

https://uwcscholar.uwc.ac.za/home

transfers and sharing; online gaming; Voice over Internet Protocol (VoIP) person-to-person communication; online social networking sites; online shopping; and news portals.

The Internet therefore operates as the hub of the personal information market by providing a tool with which to aggregate and consolidate information and aid the peddling and purchase of personal information.[97] Moreover, the Internet makes it possible to collect, record, and analyse personal data pertaining to browsing patterns and purchases made across multiple websites that is detailed, computer-processable, indexed, and permanent.[98] Due to the interactive nature of web pages, the personal data so collected may be used for the purposes of targeting, which allows for personalised advertisements.[99] Goldfarb and Tucker explain that targeting involves an advertiser choosing to display an advertisement to a specific group or particular subset of potential viewers rather than to everyone using the platform.[100]

The core of such marketing involves the exploitation of personal data. These advertisements drive e-commerce and generate much of the growth and revenue of technology companies. This inevitably raises questions as to who owns that data, the individual with whom it is associated, or the company that dedicates resources to extracting value from such data, thus sparking debates about property rights in personal data. This aspect will be discussed further in chapter four.

UNIVERSITY of the
WESTERN CAPE

2.2.3 Cloud computing

Another internet-related development relevant to personal data processing is 'cloud computing'.[101] There is no singular definition of the term 'cloud computing'. For present purposes, cloud computing may be described as technical arrangements using a network of remote servers hosted on the Internet and under the control of third parties to store, manage, and process data instead of a local server or hard drive on a personal computer.[102]

---

[97] Solove D 'Privacy and power: Computer databases and metaphors for information privacy' (2001) 53 *Stanford Law Review* 1393 1409.
[98] Kang J 'Information privacy in cyberspace transactions' (1998) 50 *Stanford Law Review* 1193 1198–99.
[99] Solove D (2001) 1410.
[100] Goldfarb A & Tucker C 'Privacy and innovation' (2012) 12 *Innovation Policy and the Economy* 65 68.
[101] Van der Merwe D et al (2016) 366.
[102] Svantesson D & Clarke R 'Privacy and consumer risks in cloud computing' (2010) 26 *Computer Law and Security Review* 391 391.

https://uwcscholar.uwc.ac.za/home

Cloud computing services are deployed in various ways, such as (1) public clouds that permit any person or entity to access the services, the control of which is managed by the cloud service provider, (2) private external clouds that restrict access to the service to only a single customer or user, the control of which is managed by the cloud service provider, (3) private internal clouds that permit organisations to use the scaling resources of cloud computing technologies while retaining full control over the cloud,[103] and (4) hybrid clouds that are a combination of the other cloud types.[104] Cloud computing services are often used for private purposes in the form of web-based email services, photo storage facilities, and social networking sites.[105] It allows for the sharing of data among devices anywhere in the world through the Internet.

With the exception of private internal clouds, all cloud computing services utilise external infrastructure provided by third parties. The level of control a data subject has over his or her data is reduced once such data is released into the cloud. Personal data may be more vulnerable to dangers from hackers, data breaches, and unauthorised transfers to third parties.[106] When cloud services are used, it is generally characterised by a shift in control over the data from the individual to the cloud service provider. The concept of control is particularly important in the US context as it is directly linked to the idea of ownership.[107] Consequently, the same question as in the previous section emerges: who owns the personal data—the individual or the company that hosts it on their servers?

Google, as an example, offers several cloud-based storage and collaboration tools, including, but not limited to, Gmail, YouTube, Google Docs, and Google Drive. To use these services, an individual must sign up for a Google account and agree to the terms and conditions of the Google privacy policy. Google does not charge users for these services; instead, the Google privacy policy provides, among other things, that Google may collect personal data such as location information, device information, IP address, and cookie data from a variety of sources,

[103] Unless the context indicates otherwise, the reference to organisations as used in this section shall imply a reference to public and private bodies, incorporated and unincorporated entities.

[104] Ruiter J & Warnier M 'Privacy regulations for cloud computing: Compliance and implementation in theory and practice' in Gutwirth S et al (eds) *Computers, privacy and data protection: An element of choice* (2011) 363–64.

[105] Privacy Rights Clearinghouse 'The privacy implications of cloud computing' 2017 available at *https://privacyrights.org/resources/privacy–implications–cloud–computing* (accessed 27 July 2020).

[106] Privacy Rights Clearinghouse 'The privacy implications of cloud computing' 2017.

[107] Lazaro C & Le Métayer D 'The control over personal data: True remedy or fairy tale?' (2015) 12 *SCRIPTed* 3 8–9.

https://uwcscholar.uwc.ac.za/home

such as mobile software applications (mobile apps),[108] browsers, and smart devices.[109] Moreover, Google may store, process, and collate the personal data using various servers located throughout the world to improve products and offerings or use the data for purposes of profiling, personalising content, and targeted advertising, which are discussed below in 2.3.3.[110] Signing up for this service illustrates the 'new' business model of exchanging personal data for access to the service. Viewed in this light, the transaction is not free despite the absence of monetary exchange. The individual 'pays' with personal data to use the service, while the service provider benefits, financially or otherwise, from the processing of such personal data.

Google's hosting of various cloud-based services creates opacity in data processing, posing a challenge for individuals to comprehend how data is processed and utilised.[111] The convoluted legal language of privacy policies leads to a lack of transparency regarding processing practices in the cloud.[112] Van den Hoven et al raise a number of privacy concerns that cloud computing presents, such as the limited understanding by a data subject as to what personal information is collected, how that information could be used, and where such information resides.[113] These privacy concerns are particularly relevant in the big data era and are discussed further under 2.3 below.

UNIVERSITY of the
WESTERN CAPE

2.2.4 Smart devices

A smart device may be defined as 'a context-aware electronic device capable of performing autonomous computing and connecting to other devices, wired or wirelessly, for data exchange'.[114] Some common 'smart devices' include smartphones, tablets, smart watches, fitness and health trackers, and smart televisions. Smart devices usually contain several data-

[108] Mobile software applications are computer programmes or software applications that are designed to run on smart devices and can be distinguished from desktop applications, which are designed to run on desktop computers, or web applications, which run in web browsers.

[109] See Google 'Privacy Policy – Privacy & Terms' (4 March 2024) available at *https://policies.google.com/privacy* (accessed 20 March 2024).

[110] See Google privacy policy.

[111] Google does disclose in its privacy policy that it uses algorithms to recognise patterns in data.

[112] Betzing J et al 'The impact of transparency on mobile privacy decision making' (2020) 30 *Electronic Markets* 607 608–9; Gürses S & Preneel B 'Cryptology and privacy in the context of big data' in Van der Sloot B, Broeders D & Schrijvers E (eds) *Exploring the boundaries of big data* (2016) 52.

[113] Van den Hoven J et al (2020) para 2.2.

[114] Silverio-Fernández M, Renukappa S & Suresh S 'What is a smart device? - a conceptualisation within the paradigm of the internet of things' (2018) 6 *Visualization in Engineering* 1 8.

https://uwcscholar.uwc.ac.za/home

generating sensors, such as cameras, motion sensors, and GPS.[115] A smart device is characterised by three features, namely:[116]

(i) autonomy, which refers to the capability of a qualifying device to perform tasks autonomously without human intervention;
(ii) connectivity, which refers to the ability of a qualifying device to connect to a data network, such as the Internet or another device on the network; and
(iii) context-awareness, which is indicative of the ability of a qualifying device to perceive information from the environment through sensor data obtained from cameras, microphones, accelerometers, and the Global Positioning System (GPS).

Smart devices such as smartphones may be characterised by their high level of integrated functionality and can be used as a phone, personal digital assistant (PDA), web browser, music player, camera, or GPS.[117] Smartphones are, increasingly, becoming an important means to obtain information, communicate and entertain. The large storage and connectivity capabilities make smartphones a personal information hub.[118] Smartphones and other mobile devices present unique privacy challenges to data subjects because they are personal to the user concerned, always on,[119] and travel with the data subject.[120] Smart devices can potentially facilitate the collection and sharing of potentially sensitive or highly personal data among various third parties.[121]

The European Union Agency for Network and Information Security (ENISA) states, with merit, that data subjects view smartphones as trustworthy, highly personal gadgets that they will not share.[122] This suggests an increasingly intimate relationship with the smart device to the extent that it has become part of the individual's identity. Polykalas et al aptly describe a

[115] Van den Hoven J et al (2020) para 2.5.
[116] Silverio-Fernández M, Renukappa S & Suresh S (2018) 5–6.
[117] Bredican J & Ellis D 'Smartphone applications – Idea sourcing, and app development: Implications for firms' (2014) 17 *SAJEMS* 232 234.
[118] Zhao B 'The internationalisation of information privacy: Towards a common protection' (2014) 2 *Groningen Journal of International Law* 1 6–7.
[119] Bredican J & Ellis D (2014) 234.
[120] FTC *Mobile Privacy Disclosures: Building Trust through Transparency* (2013) 2 available at *https://www.ftc.gov/sites/default/files/documents/reports/mobile–privacy–disclosures–building–trust–through–transparency–federal–trade–commission–staff–report/130201mobileprivacyreport.pdf* (accessed 11 February 2021).
[121] FTC *Mobile privacy disclosures: Building trust through transparency* (2013) 2.
[122] European Union Agency for Network and Information Security *Privacy and data protection in mobile applications - A study on the app development ecosystem and the technical implementation of GDPR* (2017) 11.

https://uwcscholar.uwc.ac.za/home

smartphone as a vault that stores valuable sensitive information.[123] It is submitted that the information stored on a smartphone may be more valuable than the device itself. A device that is stolen, damaged, or lost can be replaced; however, data that is lost cannot be retrieved unless there is a copy from which it can be restored. Value, as it applies to data, may not necessarily refer to monetary value but could also refer to sensitive, confidential or sentimental value. This serves to demonstrate that value can also be attributed to intangible interests such as information.

In addition to using smart devices for email, Internet browsing, and similar traditional internet services, data subjects are increasingly using such devices to acquire and download software programmes, more commonly known as 'mobile apps'.[124] Data subjects are required to grant these mobile apps various permissions to access location information, photos, media, files, Wi-Fi connection information, and identity information.[125] In this context, permissions regulate how mobile apps interact with system and device functionalities.[126] Mobile apps can potentially access large amounts of personal information stored on smartphones and send it to cloud servers, giving rise to privacy concerns.[127] Location tracking, accessing a device's contact list, recognising a phone's unique identifier, logging in-app transactions, and exchanging data with analytics organisations and marketers are examples of data that may be gathered and shared by mobile apps.[128]

Mobile app business models are almost entirely driven by the acquisition and analysis of personal data for the purposes of creating user profiles and targeting advertising.[129] While some mobile apps are based on pricing models such as on-time payment for their usage or in-app purchases for additional features,[130] the 'free' business model of providing content and services in exchange for the collection and analysis of personal information is the most lucrative option for conducting business online.[131] On one hand, 'lucrative' refers to the potential of a free app

[123] Polykalas S et al *Mobile apps and data privacy: when the service is free, the product is your data* (2017) 1.
[124] Polykalas S & Prezerakos G 'When the mobile app is free, the product is your personal data' (2019) 21 *Digital Policy, Regulation and Governance* 89 89.
[125] Polykalas S & Prezerakos G (2019) 95.
[126] See Polykalas S & Prezerakos G (2019) 95 for a list of the most common mobile app permissions.
[127] Jin H et al '"Why are they collecting my data?": Inferring the purposes of network traffic in mobile apps' (2018) 2 *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1 1–2.
[128] Sipior J, Ward B & Volonino L 'Privacy concerns associated with smartphone use' (2014) 13 *Journal of Internet Commerce* 177 180.
[129] Zarsky T 'The privacy-innovation conundrum' (2015) 19 *Lewis & Clark Law Review* 115 163; Polykalas S & Prezerakos G (2019) 90, 99.
[130] European Union Agency for Network and Information Security (2017) 33.
[131] Zarsky T (2015) 164.

https://uwcscholar.uwc.ac.za/home

to attract a significant user base and then convert those users into paying clients. On the other hand, 'lucrative' may also denote the ability to collect large volumes of personal data to generate revenue from target advertising.

Smart devices play a significant role in facilitating the commodification of personal information. They have become indispensable accessories for many individuals. Unsurprisingly, smart devices have the potential to significantly impact and transform society through increased levels of connectedness, computing power and complex decision-making, making such devices the focal point for innovation on the one hand but also raising privacy concerns on the other. Smart devices are capable of autonomous decision-making using data gathered from different sensors and predict future behaviour that could potentially violate privacy.

2.2.5 Internet of things (IoT)

Multiple definitions of IoT exist.[132] Ziegeldorf, Morchon, and Wehrle describe IoT as an 'evolution of the Internet'.[133] The Internet Society defines IoT as 'scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention'.[134] IoT also includes 'ambient intelligence', which refers to the capacity of IoT to sense the environment and the presence of users and act in accordance with such information.[135] Having regard to the technologies referred to the in the preceding sections,[136] IoT can be explained as a network of smart devices that collect and transmit data for storage, processing, and analysis using cloud computing.

The concept of IoT intelligently connects four elements, namely individuals, processes, things, and data.[137] Individuals may either be the data subjects (that is, the objects of data collection

[132] Cunningham M 'Next generation privacy: The internet of things, data exhaust, and reforming regulation by risk of harm' (2014) 2 *Groningen Journal of International Law* 115 136; Maple C 'Security and privacy in the internet of things' (2017) 2 *Journal of Cyber Policy* 155 156.

[133] Ziegeldorf J, Morchon O & Wehrle K 'Privacy in the internet of things: Threats and challenges' (2013) 4 *Security and Communication Networks* 2728 2728.

[134] Internet Society *Internet Society Policy Brief: IoT Privacy for Policymakers* (2019) 2.

[135] Purtova N 'Property in personal data: Second life of an old idea in the age of cloud computing, chain informatisation, and ambient intelligence' in Gutwirth S et al (eds) *Computers, Privacy and Data Protection: an Element of Choice* (2011) 44.

[136] See 2.2.2–2.2.4 above.

[137] Maple C (2017) 158.

https://uwcscholar.uwc.ac.za/home

by things) or they may be the recipients of data.[138] In this context, 'things' are everyday objects augmented by sensors, actuators, and other information communication technologies to enable the collection, processing, and transmission of data about themselves and their interactions with other things and individuals.[139] Processes ensure that the right information is delivered to the right person or machine at the right time.[140] Data is analysed and processed to create useful information for intelligent decision-making and control mechanisms.[141]

Potential benefits of IoT include, but are not limited to, enhancing health and safety, making industrial processes less expensive and more efficient, enhancing consumer entertainment experiences, saving energy, and supporting individuals with time management.[142] Maple comments, with some merit, that using the capabilities of IoT to collect, process, and analyse data will result in intelligent decision-making and increased efficiencies and benefits.[143] Such decision-making implies that it is done independently of human intervention. These benefits are possible due to the proliferation of IoT technologies being introduced into the human environment and incorporating a greater number of sensors and more computer processing at a decreasing cost, allowing for the continuous monitoring of activities, behaviours, speech, health, and emotions.[144] These sensors and processes are characterised by their ever-shrinking size,[145] and are integrated into various everyday objects capable of monitoring actions and behaviours that generate vast amounts of personal data.[146]

The rise in the number, variety, and proximity of sensors to data subjects' bodies and private spaces enables an escalation in the monitoring of human activity, movements and habits, which increasingly threatens privacy.[147] IoT technologies facilitate the passive collection of data as a

[138] Ziegeldorf J, Morchon O & Wehrle K (2013) 2730.
[139] Ziegeldorf J, Morchon O & Wehrle K (2013) 2729–30.
[140] Banafa A 'The internet of everything (IoE)' 29 August 2016 available at *https://www.bbvaopenmind.com/en/technology/digital–world/the–internet–of–everything–ioe/* (accessed 6 August 2020); i-SCOOP 'What the internet of everything really is – a deep dive' available at *https://www.i–scoop.eu/internet–of–things–guide/internet–of–everything/* (accessed 6 August 2020).
[141] Maple C (2017) 158.
[142] Rosner G & Kenneally E *Privacy and the Internet of Things: Emerging Frameworks for Policy and Design* (2018) 6.
[143] Maple C (2017) 159–65. Maple provides further examples of other industries that may benefit from IoT such as autonomous vehicles, logistics, smart grid technology, and agriculture.
[144] Rosner G & Kenneally E (2018) 6; Internet Society (2019) 4–5.
[145] See the reference to minitiarisation in 2.2.1 above.
[146] Ciani J 'Governing data trade in intelligent environments: A taxonomy of possible regulatory regimes between property and access rights' in Chatzigiannakis I et al (eds) *Intelligent Environments* vol 23 (2018) 287.
[147] Rosner G & Kenneally E (2018) 7.

https://uwcscholar.uwc.ac.za/home

by-product of other activities without the data subject being aware of such collection.[148] Traditionally, data subjects could exercise a measure of control over their privacy by retreating to their homes, closing an office door, or ending a telephone call; on the other hand, the sensors and always-on technology of IoT devices will increasingly erode the boundary between private and public spheres.[149] Consequently, passive collection by IoT devices poses challenges for the consent mechanism, a fundamental aspect of data protection laws like POPIA and the GDPR.

2.3 PRIVACY CHALLENGES

The use of big data technologies will inevitably result in the increased collection of personal information combined with the ever more sophisticated analysis of such information. Solove notes that processing activities involving personal information are longstanding, problematic issues typically associated with 'privacy'.[150] Similarly, Roos states that it is generally recognised that the processing of personal information constitutes a danger to a person's privacy.[151] It ought to be noted that the EU distinguishes between the right to privacy and the right to data protection.[152] Therefore, processing activities concerning personal information are generally associated with data protection from an EU perspective and may not always implicate privacy interests depending on the nature or sensitivity of the personal information.

Solove makes the point that while the processing of personal information is understood as a privacy concern, the nature of the problems is dependent on how such privacy concerns are conceptualised.[153] This requires an understanding of, among other things, how such concerns develop, how they are connected, and what it is they threaten.[154] For example, data protection regulations were enacted to ensure the lawful processing of personal information and safeguard privacy. Its purpose is not meant to facilitate the commodification of personal information. To properly conceptualise the problem, one must determine if it is just related to privacy or if it

[148] Cunningham M (2014) 133–34.
[149] Rosner G & Kenneally E (2018) 8–9. Rosner and Kenneally states that private spaces refer to both physical space and personal space, including human bodies. See also Internet Society (2019) 2–5.
[150] Solove D *The Digital Person: Technology and Privacy in the Information Age* (2004) 6.
[151] Roos A 'Core principles of data protection law' (2006) 39 *The Comparative and International Law Journal of Southern Africa* 102 105.
[152] See 3.4 and 5.3.1 below.
[153] Solove D (2004) 6.
[154] Solove D (2004) 6.

https://uwcscholar.uwc.ac.za/home

encompasses more than just privacy. Since the problem involves personal information, privacy and data protection would be the logical starting point.

Privacy challenges are many and varied. The following subsections analyse those challenges using a personal data flow model articulated by Tal Zarsky.[155] Even though references may be made to certain privacy concepts in the subsections below, a detailed examination of the notion of privacy will be carried out in chapter three. Therefore, any such references will be made, where necessary, for purposes of context to discuss privacy challenges.

2.3.1 The challenge of big data for personal Information

Big data technologies facilitate 'Knowledge Discovery in Databases' (KDD) or 'data mining', as it is more commonly known, which was first defined by Fayyad, Piatetsky-Shapiro, and Smyth as 'the nontrivial extraction of implicit, previously unknown, and potentially useful information from data'.[156] Data mining enables businesses to search for hidden patterns, trends, and associations in databases to learn more about their customers and make better business decisions.[157] This suggests that without employing big data technologies, these patterns, trends, and inferences are imperceptible to human beings.

Bentley remarks that finding these behavioural patterns will become as important as the data itself.[158] These patterns help extract valuable knowledge and insights for decision-making, similar to refining raw oil into a usable product for commercial gain. Following this analogy, it may be argued that big data technologies help facilitate the transformation of personal data, which is a reflection of identity and personhood, from being perceived as something that cannot

[155] Zarsky T 'Desperately seeking solutions: Using implementation-based solutions for the troubles of information privacy in the age of data mining and the internet society' (2004) 56 *Maine Law Review* 13 13–59. See also Zarsky T 'Transparent predictions' (2013) 4 *University of Illinois Law Review* 1503 1521. Zarsky, usefully, distinguishes three stages of the personal information flow, namely, collection, analysis, and the implementation of the data to identify challenges arising from processing activities relating to data mining of personal information. The three-stage model proposed by Zarsky is a variation of the more traditional taxonomy associated with the processing of personal information in a digital context. In this regard, see Solove D 'A taxonomy of privacy' (2006) 154 *University of Pennsylvania Law Review* 477 477–560. Zarsky's model was selected to deal with the current legal and technological landscape rather than Solove's taxonomy, as the latter is based on tort, which, as discussed in chapter four, is not effective in dealing with privacy challenges occasioned by big data technologies.

[156] Fayyad U, Piatetsky-Shapiro G & Smyth P 'From data mining to knowledge discovery in databases' (1996) 17 *AI Magazine* 37 40–1.

[157] Zarsky T (2004) 14.

[158] Bentley D 'Timeless principles of taxpayer protection: How they adapt to digital disruption' (2019) 16 *eJournal of Tax Research* 679 698.

https://uwcscholar.uwc.ac.za/home

be commoditised to something marketable. Zarsky states that the increased use of data mining to analyse personal data will create more opportunities to abuse data, and therefore it is necessary to have a clear understanding of the personal information flow and the problems that may arise at each stage of the personal information flow, namely the collection, analysis, and implementation of data.[159] The ensuing discussion will address those challenges according to the stages in the personal data flow based on Zarsky's theoretical model.

2.3.2 Collection: secrecy and consent

Zarsky defines 'collection' of personal data as the initial stage in the information flow process and often involves the first set of actions that affect an individual's privacy. Personal information can be collected directly from the individual, indirectly through surveillance and tracking, or by employing advanced algorithms to merge data from many sources and enhance the existing knowledge about the individual.[160] Nowadays, data subjects cannot participate in online activities without sharing or disclosing personal data, whether it is revealed voluntarily, consciously or otherwise.[161] It is widespread practice for businesses to use big data technologies to compile huge databases by harvesting information from many different sources to generate new personal data about data subjects by drawing inferences and making predictions about their preferences and behaviours based on such information.[162] Amazon, for instance, owns a patent for an 'anticipatory shipping' system that can predict, pack, and ship products before such products are purchased by its customers based on previous purchases, consumer behaviour, and other personal data that it collects from its interactions with customers, in addition to data collected from external datasets such as census data.[163] These techniques depend on data analytics. It is reasonable to expect that some consumers may object

[159] Zarsky T (2004) 15. Zarsky states that having an understanding of the information flow paradigm will assist in identifying the problems that could arise at each stage. Zarsky's theoretical model does have limitations in that problems or concerns may be applicable or relevant to more than one stage.

[160] Freedman M 'How and why businesses collect your personal data' *Business News Daily* 17 June 2020 available at *https://www.businessnewsdaily.com/10625–businesses–collecting–data.html* (accessed 25 February 2021).

[161] Mai J 'Big data privacy: The datafication of personal information' (2016) 32 *The Information Society* 192 192–93.

[162] Mundie C 'Privacy pragmatism: Focus on data use, not data collection' (2014) 93 *Foreign Affairs* 28 31; Paterson M & McDonagh M 'Data protection in an era of big data: The challenges posed by big personal data' (2018) 44 *Monash University Law Review* 1 3.

[163] Spiegel J et al 'Method and system for anticipatory package shipping' available at *https://patents.google.com/patent/US8615473B2/en* (accessed 25 February 2021).

https://uwcscholar.uwc.ac.za/home

to getting unsolicited items, even if such items match their likes, because they never consented to enter into such transactions.

Given the proliferation of indirect data collection stemming from the rise in the number of smart devices and the emergence of IoT, it is unlikely that data subjects will know what personal data is collected, who controls it, and the purpose for which it is used.[164] Personal data, such as web browsing and location information, increasingly originates passively from smart devices without the data subject being made aware of the data being collected or the decisions regarding the use of such data.[165] Zhao points out that new technologies threaten privacy by making mass surveillance possible on a scale that has hitherto not been envisaged, and the collapse of the separation between what is deemed public and private leads to a dilution and loss of the boundaries of private life.[166] The use of big data technologies calls for a rethink as to how privacy is conceptualised to ensure that it remains relevant and fit for purpose. This calls for a paradigm shift that takes into account legal frameworks other than privacy and data protection, such as property rights, to recognise the increasing acceptance of personal data as an economic asset.

Privacy is traditionally understood in terms of notions such as secrecy, solitude, security, and confidentiality.[167] Such a conception of privacy is aligned to Warren and Brandeis' understanding of privacy as the 'right to be let alone'.[168] However, in the context of big data, privacy is not limited to secrets alone.[169] Privacy may be invaded by big data technologies despite no secrets being revealed or embarrassing facts about individuals being disclosed.[170] The disclosure of personal information, such as location data, IP address, gender, age, web browsing history, and health information, from a mobile app does not, ostensibly, represent embarrassing facts. Individually, each item of information may look relatively innocuous or insignificant and, depending on the context, may not necessarily constitute personally identifiable information, as it may be difficult to associate a single piece of information with a

[164] Cunningham M (2014) 117.
[165] Cunningham M (2014) 143.
[166] Zhao B (2014) 9. See also Poullet Y 'Data protection legislation: What is at stake for our society and democracy?' (2009) 25 *Computer Law & Security Review* 211 213.
[167] Tavani H 'Informational privacy: Concepts, theories, and controversies' in Himma H & Tavani H (eds) *The Handboook of Information and Computer Ethics* (2008) 132–33.
[168] Warren S & Brandeis L 'The right to privacy' (1890) 4 *Harvard Law Review* 193 193–195. See 3.2.1 below for a discussion on the privacy-as-secrecy paradigm.
[169] Executive Office of the President (2014) ix.
[170] Solove D (2001) 1440.

https://uwcscholar.uwc.ac.za/home

specific individual. All these types of information are being collected continuously, without human intervention, by smart or IoT devices, with the data subject often, though not always, unaware of the actual particulars of the information being collected.

The collection of personal data is ubiquitous and an inevitable consequence of using the Internet through a computer or a smartphone.[171] Turow, Hennessy, and Draper describe this sense of inevitability as a feeling of resignation on the part of data subjects who believe that it is futile to manage or control what information businesses collect from them.[172] Mundie does not necessarily consider the ubiquitous personal data collection in the big data era an invasion of privacy, as it is generally commonplace, but articulates the problem as data subjects having no knowledge of who possesses data related to them and how such data is being used.[173] I agree with the views of the abovementioned authors. It is reasonable to argue that many people may be desensitised to the feelings of resignation when their personal data is collected due to the appeal of receiving 'free' products and services. These individuals accept that the collection of personal data is standard practice despite not being aware of how their data will be used.

Big data therefore demands a shift from the conventional approach to data protection, which centres on data collection and the consent of the individual. Cunningham states that the law fails to account for IoT in that passive data collection is now the predominant method of collecting personal data and does not rely on users having to consent to such collection.[174] The World Economic Forum mentions that it would be problematic to engage individuals for consent to collect data that they know nothing about and the use of which is yet to be determined.[175] The collection of personal information in the big data era has become the norm, and therefore concern should be directed at whether the information so collected is being analysed responsibly.[176]

UNIVERSITY of the
WESTERN CAPE

[171] Rosner G & Kenneally E (2018) 7.
[172] Turow J, Henessy M & Draper N *The Tradeoff Fallacy – How Marketers Are Misrepresenting American Consumers and Opening Them up to Exploitation* (2015) 3.
[173] Mundie C (2014) 31–2.
[174] Cunningham M (2014) 141.
[175] World Economic Forum & Kearney A *Rethinking Personal Data: A New Lens for Strengthening Trust* (2014) 10.
[176] Mai J (2016) 194.

https://uwcscholar.uwc.ac.za/home

2.3.3 Analysis of personal data: predictive analysis, profiling, and power asymmetry

> 'Analytics is what makes big data come alive. Without analytics, big datasets could be stored, and they could be retrieved, wholly or selectively. But what comes out would be exactly what went in. Analytics, comprising a number of different computational technologies, is what fuels the big-data revolution. Analytics is what creates the new value in big datasets, vastly more than the sum of the values of the parts.'[177]

'Analysis' is the second stage in Zarsky's theoretical model of personal information flow. The World Economic Forum comments that analytics is now the engine of economic and social value creation.[178] Analytics enable the transformation of raw data into meaningful insights and inferences that enable businesses to make better decisions and identify new opportunities.[179] In other words, data is transformed into a commodity and a valuable asset.

The traditional approaches to regulating privacy are premised on personal information being collected directly from the data subject and the data processing being limited to the primary purposes of its collection.[180] Big data analysis involves secondary uses of data that were not anticipated at the time that the data was collected.[181] Moreover, big data analytics use artificial intelligence and complex mathematical algorithms to analyse large datasets by seeking correlations to produce new insights and predictions that could not be anticipated prior to analysis; this may then be used to facilitate a range of decisions and activities relating to individuals and groups.[182] Much of the focus is no longer on the individual but rather on the analysis of data based on patterns and correlations among groups of individuals.[183] Correlations may suggest ways of directing activities at individuals to influence and manipulate their behaviour and inform decisions.[184] By analysing individual behaviours, preferences, and other characteristics, the individual is clustered into groups that allow for predictions and decisions

---

[177] Executive Office of the President (2014) 24.

[178] World Economic Forum *Unlocking the value of personal data: from collection to usage* (2013) 7.

[179] Inferences or 'inferred' data may be distinguished from raw or 'observed' data in that the former relates to predictions or assumptions drawn from the observed data.

[180] King N & Forder J 'Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data' (2016) 32 *Computer Law & Security Review* 696 699.

[181] Zarsky T (2004) 28; Lenard T & Rubin P *The big data revolution: Privacy considerations* (2013) 6.

[182] Paterson M & McDonagh M 'Data protection in an era of big data: The challenges posed by big personal data' (2018) 44 *Monash University Law Review* 1 3; EC *Big Data Interoperability Analysis* (2018) 2.

[183] Taylor L, Floridi L & Van der Sloot B 'Introduction: A new perspective on privacy' in Taylor L, Floridi L & Van der Sloot B (eds) *Group Privacy: New Challenges of Data Technologies* vol 126 (2017) 5.

[184] Paterson M & McDonagh M (2018) 4.

https://uwcscholar.uwc.ac.za/home

to be made at a group level rather than an individual level.[185] Taylor notes that even though individual data is aggregated with the data of others, the aggregated data may still reflect the behaviour and activities of those specific individuals.[186]

According to Pappas et al, big data analytics have evolved to such an extent that they are used by various organisations to analyse and predict phenomena such as stock prices, purchase behaviour, voting intentions, in order to influence and manipulate the perceptions, attitudes, and behaviours of data subjects by targeting them with specific information gleaned from the insights generated by big data analytics.[187] The *Facebook-Cambridge Analytica* breach is an example of how big data analytics was used to target data subjects and manipulate their political opinions. In March 2018, it was reported that the data of millions of Facebook users was improperly used by *Cambridge Analytica* to influence the 2016 US elections.[188] The facts are, briefly, that researchers paid thousands of Facebook users to take a personality test using a free app that was available on the Facebook platform.[189] Users were informed that the personal data provided would be used for academic purposes only.[190] Facebook policies at the time allowed apps to access the data of users who not only directly consented to their information being collected but also the data of other individuals in those users' social network, more commonly known as 'Facebook friends'.[191] Approximately 270 000 Facebook users downloaded the app, while an additional 50–65 million Facebook profiles were subsequently improperly shared with

[185] Mittelstadt B 'From individual to group privacy in big data analytics' (2017) 30 *Philosophy & Technology* 475 476.

[186] Taylor L, Floridi L & Van der Sloot B *Group privacy: New challenges of data technologies* (2017) 3.

[187] Pappas I et al 'Big data and business analytics ecosystems: Paving the way towards digital transformation and sustainable societies' (2018) 16 *Information Systems and e-Business Management* 479 480.

[188] Cadwalladr C & Graham-Harrison E 'Revealed: 50 Million Facebook profiles harvested for Cambridge Analytica in major data breach' *The Guardian* 17 March 2018 available at *https://www.theguardian.com/news/2018/mar/17/cambridge–analytica–facebook–influence–us–election* (accessed 27 February 2021); Rosenberg M, Confessore N & Cadwalladr C 'How Trump consultants exploited the Facebook data of millions' *The New York Times* 17 March 2018 available at *https://www.nytimes.com/2018/03/17/us/politics/cambridge–analytica–trump–campaign.html* (accessed 27 February 2021).

[189] Rehman I 'Facebook-Cambridge Analytica data harvesting: What you need to know' (2019) *Library Philosophy and Practice* 1 4.

[190] Hu M 'Cambridge Analytica's black box' (2020) *Big Data and Society* 1 2.

[191] Rehman I (2019) 5.

https://uwcscholar.uwc.ac.za/home

Cambridge Analytica.[192] *Cambridge Analytica* used the data for purposes of voter profiling and targeting to influence and manipulate the outcome of the 2016 US presidential election.[193]

It is clear that big data analytics facilitate the pervasive and potentially intrusive profiling of data subjects through the aggregation and analysis of seemingly innocuous pieces of information to create profiles or reveal sensitive personal attributes of data subjects.[194] Due to the detailed and valuable insights that inferred data can provide relating to individual data subjects and groups, these businesses tend to exercise confidentiality or assert intellectual property claims such as copyright or database rights over the inferred data that they possess on the basis of the time, energy and resources so invested.[195] Consequently, individuals are not privy to the information that a business may hold about them or how such information is used, nor do they fully comprehend the value of such information even if they were to receive free products or services in return.[196] This reflects an information asymmetry that favours businesses over individuals.[197]

In the *Facebook-Cambridge Analytica* case, data subjects were compensated for providing their personal data, but it may be argued that they are unaware of the true cost of acquiring products and services that are offered at no monetary cost. The same argument holds true for all "free" online products and services. Strandburg states, with merit, that consumers are reasonably able to determine the potential benefit or disadvantage they will incur when participating in ordinary sale transactions.[198] In contrast, the opacity of data processing in online transactions makes it difficult for them to do the same.[199] Consumers cannot properly assess the probability of harm occurring because they do not know how their information is being used, nor can they assess the magnitude of loss because they are not aware of how much

[192] FTC *Cambridge Analytica, LLC: Opinion of the Commission* (2019) 7. See also Facebook 'An update on our plans to restrict data access on Facebook' available at *https://about.fb.com/news/2018/04/restricting–data–access/* (accessed 28 February 2021).

[193] Paterson M & McDonagh M (2018) 8; Baik J 'Data Privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA)' (2020) 52 *Telematics and Informatics* 1 1.

[194] Privacy International 'Big data' (8 February 2018) available at *http://privacyinternational.org /explainer/1310/big–data* (accessed 24 August 2020); King N & Forder J (2016) 700.

[195] World Economic Forum & Kearney A (2014) 17.

[196] Haynes P & Carolyn Nguyen M 'Rebalancing socioeconomic asymmetry in a data-driven economy' in Bilao-Osorio B, Dutta S & Lanvin B (eds) *The Global Technology Report 2014: Rewards and risks of big data* (2014) 69.

[197] World Economic Forum & Kearney A (2014) 10.

[198] Strandburg K 'Free Fall: The online market's consumer preference disconnect' (2013) 13 *University of Chicago Legal Forum* 95 95–6.

[199] Strandburg K (2013) 96.

https://uwcscholar.uwc.ac.za/home

of their data is obtained or the nature of such data.[200] Therefore, data subjects often become aware of the 'true' price of the transaction when potential harms to their privacy begin to materialise. It is reasonable to argue that the individuals' loss of autonomy is part of the price to be paid in such transactions. Opaque data processing shifts power from data subjects to data collectors thereby undermining autonomy of individuals.[201] The loss of autonomy manifests in the use of influence and manipulation to shape and adjust the behaviour of individuals, thereby disregarding their individuality and their right to choose. Data subjects are effectively treated as objects for analysis.[202] It is submitted that big data accordingly objectifies data subjects by undermining their dignity, treating them as things, and disregarding their choices and feelings as to how their personal information ought to be used and processed.[203]

2.3.4 Implementation

The final stage in the data flow model is the implementation of personal information, which relates to the use of the personal information after its collection and analysis. The analysis of personal information provides opportunities for it to be used and reused, often in ways that were not foreseeable at the time that the information was collected. The concerns related to the use of big data largely stem from the ability to profile data subjects, re-identify data subjects based on supposedly anonymous information, target consumers, and discriminate among individuals. The following subsections will examine specific examples of how such information can be used, often to the detriment of the data subject.

2.3.4.1 Profiling

Big data technologies, comprising hardware such as sensors, biometrics, and computer processors, integrated with software such as data cleansing, data aggregation, and data mining techniques, allow for the creation and application of profiles.[204] A profile is a collection of

[200] Berger D 'Balancing Consumer Privacy with Behavioral Targeting' (2010) 27 *Santa Clara High Technology Law Journal* 3 24–5.
[201] Paterson M & McDonagh M (2018) 7; Jerome J 'Big data: Catalyst for a privacy conversation' (2014) 48 *Indiana Law Review* 213 216–17.
[202] Paterson M & McDonagh (2018) 7; White House *Big data: Seizing opportunities, preserving values* (2014) 41.
[203] Paterson M & McDonagh M (2018) 7.
[204] Hildebrandt M *Profiling the European citizen: Cross-disciplinary perspectives* (2008) 17–8.

https://uwcscholar.uwc.ac.za/home

information that identifies various attributes of a person, such as geographical location, group membership, interests, preferences, views, and credentials.[205] These attributes or characteristics may distinguish one person or group from another.[206]

Automated profiling is often used in the IoT environment to make decisions without the need for human intervention.[207] For example, big data and machine learning can be used to inform or determine a consumer's risk profile, particularly for financial and insurance purposes, by analysing health-related and behavioural data captured through smart wearables.

Profiling through data mining employs algorithms to discover hidden patterns and correlations and therefore does not require a hypothesis to commence the analysis, making the results unpredictable to both the person analysing the data and the person or group from whom it was collected.[208] Consequently, profiling creates added value in the mass of data by filtering out the noise from the information.[209] Notwithstanding the value of data mining, the interpretation of big data analysis remains important, as the data required for analysis may contain errors resulting in correlations that may not be appropriate for predicting outcomes or behaviours.[210] Data mining may be contrasted with traditional statistical analysis, which requires the formulation of a hypothesis against which to test the available data.[211] Profiling by means of data mining generates hypotheses itself.[212] This is so because it cannot be determined in advance what patterns or relationships, if any, will be discovered. In other words, such profiling cannot be approached with a set of pre-determined questions in mind.

Profiling can apply to either an individual or a group of people. An individual profile can identify a person and describe a set of attributes specific to that individual.[213] The contents of the profile may be collected directly from the individual, or they may be inferred or mined by

---

[205] Hasan O et al 'A discussion of privacy challenges in user profiling with big data techniques: The EEXCESS use case' (2013) *IEEE International Congress on Big Data* 25 25.

[206] De Hert P & Lammerant H 'Predictive profiling and its legal limits: Effectiveness gone forever?' in Van der Sloot B, Broeders D & Schrijvers E (eds) *Exploring the boundaries of big data* (2016) 146.

[207] Hildebrandt M *Profiling the European Citizen: Cross-Disciplinary Perspectives* (2008) 18.

[208] Zarsky T (2004) 27–8.

[209] Hildebrandt M 'Profiling and the rule of law' (2008) 60.

[210] Hildebrandt M *Profiling the European Citizen: Cross-Disciplinary Perspectives* (2008) 18 explains that correlations indicate a relation between data, without establishing causes or reasons. See also White House (2014) 7.

[211] Hildebrandt M 'Profiling: From data to knowledge' (2006) 30 *Datenschutz und Datensicherheit – DuD* 548 548; Custers B 'Data dilemmas in the information society: Introduction and overview' in Custers B et al (eds) *Discrimination and Privacy in the Information Society. Studies in Applied Philosophy, Epistemology and Rational Ethics* vol 3 (2013) 5; De Hert P & Lammerant H *Exploring the Boundaries of Big Data* (2016) 146.

[212] Custers B (2013) 14.

[213] Hildebrandt M (2006) 549.

https://uwcscholar.uwc.ac.za/home

a service that manages the profile.[214] Regarding individual profiling, individuals lack control over the processing of their personal information and are uninformed about how their information is processed and transferred between systems. Big data analytics may be used to aggregate and analyse existing publicly available information to generate predictive profiles that have a high probability of being classified as personal information, thereby increasing the amount of related data that could be considered private.[215] Such profiling can reveal very sensitive and intimate information that could be shared with third parties without the knowledge of the individuals concerned.

A group profile identifies and represents a group of individuals who share a set of attributes.[216] Attributes may include age, gender, religion, income, credit history, lifestyle behaviours, level of education and location. Hildebrandt explains that a group may consist of either a community of individuals, which may be an existing group, or a category of individuals that have no connection among themselves but that are established through profiling.[217] Group profiling may be further distinguished between distributive and non-distributive profiles. A distributive profile is when all the members of the group share the same attributes, while a non-distributive profile represents a group that does not share the same attributes except for a statistical relationship.[218] In the case of non-distributive profiling, the profile is inferred from large amounts of often anonymised data relating to many other individuals.[219] A non-distributive profile may be valid for a group and for individuals as members of that group, but not for individuals as such.[220] Some individuals may, therefore, share certain attributes with other members of that group, but not all of the attributes.

Group profiling, specifically non-distributive profiling, creates opportunities for individuals to be profiled without the need to be identified. Individuals' common risks and behaviours are of greater interest than the individuals themselves.[221] Such profiling is not dependent on the

---

[214] Hasan O et al (2013) 26.

[215] Crawford K & Schultz J 'Big data and due process: Toward a framework to redress predictive privacy harms' (2014) 55 *Boston College Law Review* 93 98.

[216] De Hert P & Lammerant H *Exploring the Boundaries of Big Data* (2016) 147.

[217] Hildebrandt M (2006) 549.

[218] Hildebrandt M *Profiling the European Citizen: Cross-Disciplinary Perspectives* (2008) 21; De Hert P & Lammerant H *Exploring the Boundaries of Big Data* (2016) 148.

[219] Andrade N 'Data protection, privacy and identity: Distinguishing concepts and articulating rights' in Fischer-Hűbner S et al (eds) *Privacy and Identity Management for Life. Privacy and Identity 2010. IFIP Advances in Information and Communication Technology* vol 352 (2010) 103.

[220] Custers B *Discrimination and Privacy in the Information Society. Studies in Applied Philosophy, Epistemology and Rational Ethics* (2013) 11.

[221] Mittelstadt B (2017) 478.

https://uwcscholar.uwc.ac.za/home

collection of personal data from an individual but rather is mined and created using the data of other individuals or groups to create a profile that may then be applied to a particular person.[222] Generalisations are then formulated based on inferences.[223]Consequently, the probability exists that such profiling may result in inaccuracies when applied to individuals resulting in a specific individual or individuals being misclassified as belonging to a certain group. Such inferences imposed on an individual who is part of that group threaten the individual's autonomy and capacity to shape and control their identity.[224] This may lead to or perpetuate existing stereotypes, discrimination and other privacy concerns.

It is clear that the commodification of personal data lies at the heart of profiling. Profiling is not limited to individuals voluntarily sharing personal data. Big data analytics and algorithms are largely responsible for the transformative effect on personal data since the collection of data occurs mostly passively. Personal data is no longer merely an aspect of identity or personhood; it is a resource that has commercial application. Big data analytics and the use of algorithms help to unlock the economic potential of personal data to the extent that it can be monetised, thus objectifying the individual. The data practices resulting from such commodification can adversely affect individuals in various ways, as is discussed below.

UNIVERSITY of the
WESTERN CAPE

2.3.4.2 Re-identification

The use of big data analytics presents opportunities to increase economic growth, benefit customers through innovative goods and services, improve government services, save lives, and so forth, which must be balanced against the risks and challenges occasioned by these technologies.[225] However, the use of big data technologies also presents privacy concerns. The challenge lies in striking a balance between the societal harms caused by big data technologies and the value derived from their insights.[226] Anonymisation has been mentioned as one of big data's built-in privacy safeguards.[227]

[222] Hildebrandt M 'Profiling and the rule of law' (2008) 62.
[223] Hildebrandt M (2006) 550.
[224] Mittelstadt B (2017) 479–80.
[225] White House (2014) 5.
[226] White House (2014) 5.
[227] Lerman J 'Big data and its exclusions' (2013) 66 *Stanford Law Review* 55 60.

https://uwcscholar.uwc.ac.za/home

Anonymisation refers to the process of eliminating all identifying elements from a set of personal data so that the data subject is no longer identifiable.[228] The term 'de-identification' has a similar meaning. The 'Working Party on the Protection of Individuals with regard to the Processing of Personal Data Working Party' (WP29)[229] further describes this anonymisation process as irreversible.[230] Some legal scholars and policymakers have promoted anonymisation and its promises to enhance the privacy of data subjects.[231] It is claimed that anonymisation may offer a strategy to reap the benefits of the technological revolution while simultaneously mitigating privacy risks by employing techniques that can provide privacy guarantees.[232] Froomkin contends that anonymity is a means of preventing profiling.[233] However, it is submitted that complete anonymity will be difficult to achieve. This is due to the sheer volume, variety and velocity of data that is available for collection and analysis. It may be argued that as technologies develop, anonymisation techniques will improve, but so will the possibilities of re-identifying data.

UNIVERSITY of the
WESTERN CAPE

Organisations generally promise data subjects anonymity in return for the use of their data.[234] Such claims or promises are made to eliminate privacy risks often associated with data handling practices by removing personal information that could reveal information about the data subject.[235] Data is regarded as anonymous if it does not contain information that can be used to identify or re-identify data subjects, in which case it is no longer considered personal

---

[228] European Union Agency for Fundamental Rights et al *Handbook on European Data Protection Law* (2018) 93.

[229] WP29 was set up under Article 29 of the General Data Protection Regulation to provide independent advice on data protection matters and was composed of a representative of each of the national supervisory authorities in the EU member states, a representative of the European Data Protection Supervisor (the authority established for the Community institutions and bodies), and a representative of the EC (the latter also provides the secretariat for the Working Party). Under the GDPR, the European Data Protection Board (EDPB) will replace WP29.

[230] WP29 *Opinion 05/2014 on Anonymisation Techniques* (2014) 6. Whereas the WP29 adopts the strict approach that anonymisation ought to be permanent, recital 26 of the GDPR follows a risk-based approach to anonymisation which states that identification must be 'reasonably impossible'.

[231] Brenner S 'Privacy privilege: Law enforcement, technology, and the Constitution' (2002) 7 *Journal of Technology Law & Policy* 123 139; Lessig L *Code Version 2.0* (2006) 45; Ohm P 'Broken promises of privacy: Responding to the surprising failure of anonymization' (2010) 57 *University of California Law Review* 1701 1710–11; Yakowitz J 'Tragedy of the data commons' (2011) 25 *Harvard Journal of Law & Technology* 1 2–3. The concept of anonymisation has also been incorporated into data protection legislation such as the GDPR and POPIA. The processing of anonymised personal information falls outside the ambit of data protection legislation. Telecommunication organisations are providing governments with anonymised datasets for the purposes of tracking and containing the COVID-19 pandemic. For more information see OECD *Tracking and Tracing COVID: Protecting Privacy and Data While Using Apps and Biometrics* (2020) 1–5.

[232] WP29 (2014) 3.

[233] Froomkin M 'From anonymity to identification' (2015) 1 *Journal of Self-Regulation and Regulation* 120 121.

[234] Taylor L 'Safety in numbers? Group privacy and big data analytics in the developing world' in Taylor L, Floridi L & Van der Sloot B (eds) *Group Privacy: New Challenges of Data Technologies* vol 126 (2017) 13.

[235] Ohm P (2010) 1703.

https://uwcscholar.uwc.ac.za/home

information.[236] The implication of this is that if information is no longer deemed personal information, then it will fall outside the ambit of data protection laws and there will be no duty or obligation to comply with such laws.

Gruschka et al contend that even if elements of personal information are removed from a dataset, additional information can be used to re-identify data subjects.[237] A well-known example of re-identification is the Netflix prize contest, which occurred in 2006.[238] The motive for the competition was to improve the accuracy of recommendations and predictions about what individuals would like to watch based on their movie preferences. Netflix released a dataset containing movie ratings from half a million customers. Netflix anonymised the records by removing information that could be used to identify individuals and replacing it with indirect identifiers, which on their own cannot be used to identify individuals. The indirect identifiers and the movie ratings were then published. Researchers combined this published data with other publicly available information to re-identify individuals.[239] The Netflix case demonstrates that seemingly harmless datasets may also pose privacy challenges and that achieving complete anonymity is a challenge.

Ohm claims, with some merit, that the faith placed in anonymisation to protect privacy is illusory due to the advances in re-identification.[240] Ohm argues further that the idea of protecting privacy by anonymising personal data should be abandoned.[241] The concept of personal information, or 'personally identifiable information', which is a central tenet in many existing data protection regimes, is threatened by re-identification.[242] In big data analytics, the

[236] See s 6(1)(b) of POPIA. See also Recital 26 of the GDPR. The GDPR distinguishes between anonymisation and pseudonymisation. WP29 (2014) 20 describes pseudonymisation as replacing a unique attribute in record by another so that re-identification is not possible without the use of additional information. Recital 28 of the GDPR regards pseudonymisation as a privacy enhancing technique, but the resultant pseudonymised data is still considered personal data.

[237] Gruschka N et al 'Privacy issues and data protection in big data: A case study analysis under GDPR' (2018) *IEEE International Conference on Big Data* 5027 5028.

[238] Author Unknown 'The Netflix Prize Rules' (undated) available at *https://netflixprize.com/assets/rules.pdf* (accessed 4 September 2020).

[239] Narayanan A & Shmatikov V 'How to break anonymity of the Netflix prize dataset' (2006) *ArXiv* 1 1–10. Other well-known cases that involve the re-identification of individuals are MIT researchers being able to identify users from a phone's location data. See De Montjoye Y et al 'Unique in the crowd: The privacy bounds of human mobility' (2013) *Scientific Reports* 1 1–5. See also Barbaro M & Jr T 'A face is exposed for AOL Searcher No. 4417749' *The New York Times* 9 August 2006 available at *https://www.nytimes.com/2006/08/09/technology/09aol.html* (accessed 4 September 2020). American On Line (AOL) release of search queries from hundreds of thousands of its users over a three month period.

[240] Ohm P (2010) 1704.

[241] Ohm P (2010) 1742.

[242] Cunningham M (2014) 127.

https://uwcscholar.uwc.ac.za/home

classification of information as 'personal' is irrelevant.[243] Organisations employ powerful algorithms to de-anonymise the data by combining it with other information, which allows for the re-identification of data subjects.[244] Big data profiling is not dependent on the collection and analysis of personal data from data subjects, as personal data may be derived from the combination and analysis of seemingly unrelated data sets that might not have presented privacy issues at the time of collection.[245] Big data undermines the delineation between personal data and non-personal data, as it may be possible to link datasets and infer personal data from seemingly non-personal data.[246] Big data poses a problem to anonymisation, that is, de-identifying personal information to the extent that it cannot be re-identified again.

2.3.4.3 Behavioural targeting

Behavioural targeting is a specific type of profiling. Behavioural targeting is also known as 'behavioural advertising', 'behavioural marketing', 'preference marketing', or 'online profiling'.[247] In this section the terms will be used interchangeably. Boerman, Kruikemeier, and Zuiderveen Borgesius define behavioural targeting as 'the practice of monitoring individuals' online behaviour and using the collected information to show them individually targeted advertisements'.[248] The purpose of behavioural advertising is to increase the relevance of the advertising displayed to data subjects and ultimately influence their purchase behaviour.[249] These behavioural advertising practices enable identified groups to be targeted with more efficient advertisements resulting in a reduction of costs for advertisers.[250] Generally, the information that is collected from data subjects cannot be used to identify them, as it does not contain elements of personal information that, on their own, can be used to do

[243] Mittelstadt B (2017) 478.
[244] Cunningham M (2014) 126–27.
[245] King N & Forder J (2016) 701.
[246] Finck M & Pallas F 'They who must not be identified-distinguishing personal from non-personal data under the GDPR' (2020) 10 *International Data Privacy Law* 11 11.
[247] Insights Association 'Behavioral Targeting' available at *https://www.insightsassociation.org/issues–policies/glossary/behavioral–targeting* (accessed 7 September 2020).
[248] Boerman S, Kruikemeier S & Zuiderveen Borgesius F 'Online behavioral advertising: A literature review and research agenda' (2017) 46 *Journal of Advertising* 363 364.
[249] Bennet S 'Regulating Online Behavioral Advertising' (2011) 44 *The John Marshall Law Review* 899 899.
[250] Goldfarb A & Tucker C (2012) 68.

https://uwcscholar.uwc.ac.za/home

so.[251] Cookie data, search history, transactions, media consumption data, social network posts, and clickstream data are some examples of data connected with online behaviour.[252]

Many consumers willingly disclose personal information to acquire free products and services in exchange for agreeing to receive targeted advertising.[253] Berger argues that consumers are not able to fully comprehend the potential risks inherent in participating in activities involving behavioural targeting because they lack accurate information about the probability of the loss and the magnitude of the harm that could occur.[254] Increasing the relevance of behavioural advertising means increased intrusiveness and less control over the use of personal information.[255] More relevant advertising means that such advertisements are more closely aligned to the interests of various consumers. It is submitted that this is possible due to more data about a specific consumer being collected and analysed to personalise the advertisements.

2.3.4.4 Discrimination

Classification and division are at the heart of predictive data mining, and discrimination is a consequence of the profiling process.[256] Big data analytics may undermine the fair and equitable treatment of individuals.[257] Through profiling, shared features and behaviours that are used to group individuals are attributed to individuals as members of the group but may be an imperfect reflection of the individual within the group.[258] These generalisations about an individual may affect his personal autonomy and potentially reinforce existing injustices and stereotypes, which may be a source of discrimination.[259]

Discrimination may affect individuals in various ways. First, automated decision-making may lead to unfair, discriminatory, or biased outcomes to the detriment of those who are already

[251] Berger D (2010) 9.
[252] Boerman S, Kruikemeier S & Zuiderveen Borgesius F (2017) 364.
[253] Mundie C (2014) 32.
[254] Berger D (2010) 24. See also 2.3.3 above.
[255] Tucker C 'The economics of advertising and privacy' (2012) 30 *International Journal of Industrial Organisation* 326 326.
[256] Custers B & Schermer B 'Responsibly innovating data mining and profiling tools: A new approach to discrimination sensitive and privacy sensitive attributes' in Van den Hoven J et al (eds) *Responsible Innovation 1: Innovative Solutions for Global Issues* (2014) 337.
[257] Mittelstadt B (2017) 480.
[258] Mittelstadt B (2017) 478–79.
[259] Hildebrandt M & Gutwirth S 'General introduction and overview' in Hildebrandt M & Gutwirth S (eds) *Profiling the European Citizen: Cross-Disciplinary Perspectives* (2008) 12.

https://uwcscholar.uwc.ac.za/home

marginalised, and secondly, inaccurate or biased data can feed into profiles, leading to discriminatory outcomes for the individuals concerned.[260] For instance, big data analytics may be used to refuse a person loans or credit advances based on their ethnicity or location of residence.[261] Countries enact laws to promote equality and prevent discrimination. In South Africa, the National Credit Act (NCA)[262] seeks, among other things, to ensure (1) consumers are better informed regarding lending practices,[263] (2) consumers are not discriminated against on the grounds as set out in s 9(3) of the Constitution,[264] and (3) consumer information is up to date.[265] Significantly, the NCA is silent regarding automated decision making,[266] which could be construed as relying on human intellect for the most part to arrive at decisions.

As big data analytics become more prevalent, the application of human intellect will gradually be replaced by automated decision-making.[267] In this regard, Gillis and Spiess note that many of the present legal requirements were created with human decision-making situations in mind, and that their efficacy would be challenged by the rising automation of decision-making based on big data analytics.[268] The perceived opportunities to exclude discrimination based on certain grounds as set out in legislation may not yield the expected outcomes in big data analytics because of the ability to use proxies for such grounds.[269] For instance, the omission of race from an algorithm may not affect the outcome of an automated decision since other characteristics such as income, education, and area of residence may be aggregated and analysed to get a comparable result. Big data can therefore be used to perpetuate harmful discrimination and inequality, which offend the values of dignity and equality underscored by the Bill of Rights in the Constitution.

---

[260] Privacy International *Data Is Power: Profiling and Automated Decision-Making in GDPR* (2018) 8.

[261] White House (2014) 53.

[262] Act 34 of 2005.

[263] Sections 3 and 13, NCA.

[264] Section 61, NCA.

[265] Section 70, NCA.

[266] Credit Bureau Association *Code of Conduct: Lawful Processing of Personal Information in Credit Sector*' (Undated) 52.

[267] The current South African legislative framework does make provision for automated decision-making. Section 71(1) of POPIA provides that the making of a decision that substantially affects the individual and is based solely on automated processing of personal information is prohibited. Section 71(2), however, provides for exceptions to the prohibition on decision-making based on automated processing, subject to appropriate measures being adopted to protect the individual's legitimate interests, such as the right to question decisions that have been made.

[268] Gillis T & Spiess J 'Big data and discrimination' (2019) 86 *University of Chicago Law Review* 459 459.

[269] Gillis T & Spiess J (2019) 467–471.

https://uwcscholar.uwc.ac.za/home

Mittelstadt states that the selection and limitations of the data used to inform algorithmic predictive models and the decision-making process are hindered by the opacity of analytics.[270] On the one hand, data subjects are not in a position to protect themselves because they do not understand how algorithmic decision-making works.[271] Data subjects will fail to understand why a particular decision was taken, the basis for such a decision, or how to interrogate the automated decision-making process.[272] Despite this, officials frequently rely on computer-generated findings because they lack the skills and knowledge to check their correctness and accuracy.[273]

2.3.4.5 Re-use and secondary uses of personal information

Data protection regimes provide for the collection and use of personal information based on consent.[274] The purpose specification condition in POPIA expressly requires that personal information be collected for a purpose that is 'specific, explicitly defined, and lawful'.[275] POPIA further stipulates that any new processing activity performed on personal information so collected must be 'adequate, relevant and not excessive'[276] and be compatible with the original purpose.[277] Similarly, the GDPR provides that personal data must be collected for a specific, explicit, and legitimate purpose and cannot be processed further in a way that is incompatible with the original purposes.[278] Furthermore, personal information processed in terms of the GDPR must be limited to what is necessary in relation to the purposes for which it is processed.[279] In the US, the Federal Trade Commission (FTC) has implemented a number of 'fair information practice principles' (FIPPs) that represent widely accepted concepts concerning the use of personal information and relate, among other things, to informed consent

[270] Mittelstadt B (2017) 481.
[271] Bruckner M 'The promise and perils of algorithmic lenders' use of big data' (2018) 93 *Chicago-Kent Law Review* 3 44–5.
[272] Custers B & Schermer B *Responsible Innovation 1: Innovative Solutions for Global Issues* (2014) 340.
[273] De Hert P & Lammerant H *Exploring the Boundaries of Big Data* (2016) 153.
[274] See POPIA and the GDPR in 3.6 and 5.3.3 respectively.
[275] See s 13, POPIA.
[276] Section 10, POPIA.
[277] Section 15(1), POPIA.
[278] Article 5(1)(b), GDPR.
[279] Article 5(1)(c), GDPR. POPIA, on the other hand, does not require that processing be necessary for a specific purpose. See 5.3.3.2.2 below.

https://uwcscholar.uwc.ac.za/home

that data subjects must provide prior to the collection and use of personal data and limiting the reuse of personal data that is incompatible with the purpose that data subjects consented to.[280]

Big data enables the repurposing of data for uses other than those for which it was originally collected. Reuse may be defined as the secondary use of data that follows its initial collection and use.[281] Policymakers recognise the opportunities for value creation through the use of big data.[282] It is further acknowledged that the value of information does not reside in the primary purpose for which it was collected but rather in the innovative secondary uses that were not envisaged when the data was first collected.[283] By aggregating large amounts of data from various sources, big data enables the discovery of novel trends, correlations, and relationships.[284]

Consumers generally lack an understanding of the extent to which personal data is processed and reused by third parties.[285] The assumption that a consumer's consent, in a big data context, is based on a conscious, rational, and autonomous choice appears flawed.[286] First, as mentioned above in 2.3.2, due to the ubiquitous nature of data collection in the big data era, consumers are often unaware that their personal data is being collected or the nature of the data being collected. Secondly, consumers often do not understand what they are consenting to, as privacy policies are often lengthy or written in vague terms that cannot be easily understood.[287] Thirdly, neither the data collector nor the data subject can reasonably be expected to know what the data will be used for.[288] Moreover, big data also undermines the idea of consent at the group level by making consent irrelevant for those individuals included in a group whose individual data did not contribute to that group profile.[289]

[280] For more information see FTC *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*' (2000) 36–8. See also 4.7.1 below.
[281] Ursic H & Custers B 'Legal barriers and enablers to big data reuse' (2016) 2 *European Data Protection Law Review* 209 210.
[282] White House (2014) 37; Ursic H & Custers B (2016) 209.
[283] Lenard T & Rubin P (2013) 6. Lenart and Rubin highlight a number of innovations derived from the secondary uses of personal data in the health and financial sectors.
[284] Custers B & Ursic H 'Big data and data reuse: A taxonomy of data reuse for balancing big data benefits and personal data protection' (2016) *International Data Privacy Law* 1 2.
[285] Altman M et al (2018) 37.
[286] Mai J (2016) 193.
[287] Altman M et al (2018) 37.
[288] Froomkin M 'Big Data: Destroyer of Informed Consent' (2019) 21 *Yale Journal of Law and Technology* 27 30.
[289] Froomkin M (2019) 33.

https://uwcscholar.uwc.ac.za/home

It is argued that in many instances involving data reuse, the legal bases for collection and purpose specification will not be used in practice.[290] Stringent data protection laws will merely impede the free flow of data and consequently compromise the growth of big data and its ensuing benefits.[291] The requirement that the collection of personal information be reasonably necessary for or directly related to the purpose is arguably inadequate when it relates to big data analytics.[292] Moreover, the data minimisation principle is described as being inimical to the underlying thrust of big data, which is to discover novel correlations through the application of analytical techniques, free of any ex ante restrictions.[293] Zarsky concludes, with merit, that although there appears to be conflict between contemporary data protection regimes and big data practices, big data analysis of personal information will become entrenched due to the innovation opportunities and the potential benefits to be derived therefrom.[294]

Secondary uses of personal data also raise questions as whether such data is susceptible to ownership. Businesses are prepared to invest heavily in the processing of personal data to obtain gains,[295] and therefore engage in secondary uses of personal data for such purposes. Moreover, it would be no surprise if businesses laid claim to such data because of the resources invested to extract potential patterns and correlations. Businesses unquestionably regard personal data as a commodity.

UNIVERSITY of the
WESTERN CAPE

2.4 CONCLUSION

This chapter examined various big data practices and the concomitant concerns regarding the processing of personal information. Converged or smart technologies facilitate the increased collection and use of personal information from multiple sources, giving rise to potential privacy issues for data subjects. Many data subjects are in a state of constant surveillance due to everyday objects fitted with sensors that are capable of recording and sharing information on human activity, leading to a blurring of what is considered public and private space. A trend that emerges from big data practices is that an individual cannot exercise proper control over

[290] Ursic H & Custers B (2016) 212.
[291] Zarsky T 'Incompatible: The GDPR in the age of big data' (2017) 47 *Seton Hall Law Review* 995 1002.
[292] Paterson M & McDonagh M (2018) 13.
[293] Rubinstein I 'Big data: The end of privacy or a new beginning?' (2013) 3 *International Data Privacy Law* 74 78.
[294] Zarsky T (2017) 1002–4.
[295] Bottis M & Bouchagiar G 'Personal data v. Big data: Challenges of commodification of personal data' (2018) 8 *Open Journal of Philosophy* 206 206.

https://uwcscholar.uwc.ac.za/home

the collection, analysis, and use of his personal information. Another development is that big data technologies can autonomously make decisions for individuals based on their surroundings with little human involvement. Such automated decision-making undermines the data subject's ability to exercise his own choice.

These technological developments have undermined privacy protection and point to shortcomings in current data protection laws. Privacy is compromised when big data practices aim to influence and manipulate individuals' conduct through behavioural advertising and targeting, putting their freedom and autonomy at jeopardy. A further concern is that big data practices may reveal private information and undermine human dignity by treating data subjects as objects for analysis. Group profiling disregards the autonomy and identity of an individual by classifying him as being part of a group, which could lead to unfair, opaque decision-making, stereotyping, and discrimination. The ubiquitous collection of personal information in the big data era undermines data subjects' right to consent to the collection and subsequent processing of their personal information.

Aside from the privacy concerns, it is precisely the big data processing cycle that facilitates the commodification of personal information. The various stages of the personal data flow model, namely collection, analysis and implementation or use, each play a pivotal role in ultimately extracting economic value from personal information. In so doing, the personal information itself becomes a commodity, much like oil that is subsequently refined to create products. The technological developments discussed in this chapter will doubtless influence the nature and scope of the right to privacy. Personal information is essential in modern data-driven business models to unlock paths to greater innovation and value generation. The purported commodification of personal information will be discussed further in chapters four, five, and six. The next chapter will examine the right to privacy in South Africa and the conceptualisation thereof in light of the impact of the big data era.

https://uwcscholar.uwc.ac.za/home

CHAPTER THREE: ASSESSING SOUTH AFRICA'S DATA PROTECTION REGIME IN LIGHT OF CURRENT PERSONAL DATA PROCESSING PRACTICES

3.1 INTRODUCTION 62

3.2 CONCEPTIONS OF PRIVACY UNDERPINNING DATA PROTECTION 64

3.2.1 Privacy-as-secrecy 66

3.2.2 Privacy-as-control 68

3.3 THE RIGHT TO THE PROTECTION OF PERSONAL INFORMATION 71

3.3.1 Common law protection 71

3.3.2. Constitutional protection 74

3.3.3 Statutory protection 79

3.4 RELATIONSHIP BETWEEN PRIVACY AND DATA PROTECTION 81

3.5 LOOKING BEYOND PRIVACY AND DATA PROTECTION 85

3.6 TRANSFORMATIVE NATURE OF THE CONSTITUTION 87

3.6.1 Transformative constitutionalism 87

3.6.2 Horizontality 88

3.6.3 Subsidiarity 92

3.7 CONCLUSION 93

https://uwcscholar.uwc.ac.za/home

3.1 INTRODUCTION

Privacy is constantly being challenged and eroded by technological developments. Given the increasing number of things embedded with sensors, electronics, and connectivity capable of collecting and transmitting data, it is practically impossible for any person to isolate themselves from the world, as technology and the sharing of personal information are essential features of modern society. Those who attempt to detach themselves face difficulties as tracking and monitoring of personal data by others remain possible.

Notwithstanding the privacy challenges, technological developments also offer opportunities for innovation.[296] The uptake of smart devices by people and the always-on technology and connectivity offered by IoTs make it possible to create and develop new business models and revenue streams from the behavioural data that is collected. The Internet has presented a platform for innovative business models such as delivering digital content and services in exchange for personal information.[297] In today's digital environment, individuals consciously and willingly, share, surrender, and disclose their personal information for a variety of reasons, including getting access to digital content, goods, services and information.[298] Eggers, Hamill and Ali opine '[p]ersonal data has an economic value that can be bought, sold and traded'.[299] Data has become a valuable resource and a catalyst for growth and change, creating new businesses and opportunities.[300] Customer databases are often a company's most valuable asset.[301] Data-driven business models and practices have enabled companies to benefit from and profit from the analysis of personal information.[302] These companies enjoy strong

[296] Zarsky T 'The privacy-innovation conundrum' (2015) 19 *Lewis & Clark Law Review* 115 117.

[297] Eggers W, Hamill R & Ali A 'Data as the new currency: Government's role in facilitating the exchange' (2013) 13 *Deloitte Review* 18 21.

[298] See 1.2 and 2.2.2.2 above. See also SALRC 'Project 124: Privacy and Data Protection Report' (2009) para 1.2.9. A further illustration is the use of free Wi-Fi services in airports, restaurants, shopping malls, and various other places, where users wishing to sign up for such a service must accept cookies and disclose personal information that may include an email address, location data, and a history of websites visited. This personal information is often shared by the WiFi service provider with third parties.

[299] Eggers W, Hamill R & Ali A (2013) 19.

[300] Strowel A 'Big data and data appropriation in the EU' in Aplin T (ed) *Research Handbook on Intellectual Property and Digital Technologies* (2020) 107.

[301] Elvy S 'Commodifying consumer data in the era of the internet of things' (2018) 59 *Boston College Law Review* 423 428.

[302] See 1.2 above.

https://uwcscholar.uwc.ac.za/home

monopolies as their 'competitive advantage is increasingly being tied to their control of the "new oil" of personal data which is sold to other businesses as a commercial asset'.[303]

Big data technologies and the use of behavioural data provide companies across various sectors of the economy with the technological foundation that is essential for innovation and economic progress.[304] Falch submits that these developments relating to the harvesting of behavioural data, which enable revenues to be generated from the use of such data, represent the emergence of a new techno-economic paradigm.[305] According to Perez, a techno-economic paradigm involves a new technological revolution that introduces a cluster of new technologies, products, and industries that disrupt existing organisational and economic practices; it requires a vast reorganization of pre-existing industries and opens up new opportunities throughout the economy.[306] As current regulatory approaches are not well-suited to support technological advancements, these technological revolutions present challenges for existing regulatory frameworks, in this case the attempts to achieve and maintain a balance between fostering innovation and protecting data subjects' privacy. Hagemann, Skees and Thierer refer to this phenomenon as the 'pacing problem', which is defined as 'the gap between the introduction of a new technology and the establishment of laws, regulations, and oversight mechanisms for shaping its safe development'.[307] Implementing an effective legal solution requires a shift in mindset to view and understand the legal problem from another viewpoint and to be open to considering alternative legal approaches.

---

[303] Cachalia F & Klaaren J *Digitalisation, the 'Fourth Industrial Revolution' and the Constitutional Law of Privacy in South Africa: Towards a Public Law Perspective on Constitutional Privacy in the Era of Digitalisation* vol 14 (2021) 13.

[304] Falch M *Surveillance Capitalism - a New Techno-Economic Paradigm* in *13th CMI Conference on Cybersecurity and Privacy (CMI) – Digital Transformation – Potentials and Challenges* (2020) 2–3. Burns Y & Burger-Smidt A *Protection of Personal Information: Law and Practice* 2 ed (2023) 789 observe that big data processing in South Africa is not as prevalent as in the US. However, this does not mean that South Africa is immune from the effects of big data processing. This is so because international companies have a presence in South Africa.

[305] Falch M (2020) 3–5. Falch states behavioural data is a key input in the emerging techno-economic paradigm.

[306] Perez C 'Technological revolutions and techno-economic paradigms' (2010) 34 *Cambridge Journal of Economics* 185 190. Perez identifies five different technology revolutions from the 1770s to the 2000s, commencing with the Industrial Revolution in 1771, followed by the steam engine in 1829, steel, electricity, and heavy engineering in 1875, automobiles and mass production in 1908, and lastly, information and telecommunications in 1971.

[307] Hagemann R, Skees J & Thierer A 'Soft law for hard problems: The governance of emerging technologies in an uncertain future' (2018) 17 *Colorado Technology Law Journal* 37 59. See also Lawack V, Kaseke M & Fransman M 'Consumer Protection Law Aspects of Cryptoassets' in Lawack V (ed) *Fintech Law and Regulation: An African Perspective* (2023) 337–40 for an example of the pacing problem encountered in consumer protection law in South Africa. Neither the Electronic Communications and Transactions Act 25 of 2002 nor the Consumer Protection Act 68 of 2008 envisage personal data as a means of exchange or payment, despite current data practices.

https://uwcscholar.uwc.ac.za/home

Challenges concerning the processing of personal information are typically characterised as matters of privacy, hence the enactment of data protection rules. Beyond privacy, however, the existing data protection regulatory environment becomes less clear when dealing with personal information as a commodity or medium of exchange. As such, it would be erroneous to think of personal information only in terms of privacy. It is therefore important to understand whether the conceptual framework underpinning the South African privacy and data protection framework adequately deals with:

a. the privacy concerns in the big data era; and
b. how personal information is treated as a commodity.

This chapter begins by exploring the various conceptions of privacy underpinning data protection. The right to privacy in South Africa is analysed insofar as it deals with the processing of personal information and to establish to what extent, if any, such conceptions are reflected in South Africa law. In so doing, the constitutional right to privacy in the context of South Africa's transformative constitution is considered within the context of privacy harms brought about by technological change. As informational privacy is a key focus area of this dissertation, the relationship between privacy and data protection is discussed. The possible shortcomings of South Africa's data protection principles are examined in the context of the big data era. This chapter is intended to lay the foundation, in the subsequent chapters, for the discussion of the propertisation of personal information as a means of acknowledging the commodification or economic value attributed to personal information.

3.2 CONCEPTIONS OF PRIVACY UNDERPINNING DATA PROTECTION

Data processing poses a threat to a person's privacy.[308] This claim is partly accurate. However, based on the problem statement outlined in chapter one and the reasons stated below,[309] it is argued that this represents a rather narrow perspective of data processing and the repercussions of such processing. When personal information is used as a medium of exchange, data processing is an inevitable consequence, which may not inherently pose a risk to privacy. The right to privacy remains relevant but may, in certain instances, only be an incidental issue.

[308] Roos A 'Core principles of data protection law' (2006) 39 *The Comparative and International Law Journal of Southern Africa* 102 105–6.
[309] See 3.5 below.

https://uwcscholar.uwc.ac.za/home

According to Schwartz, data processing could potentially suppress individual self-determination and free choice and states 'the more that is known about an individual, the easier it is to force his obedience. Through the use of their data banks, the state and private organizations can transform themselves into omnipotent parents and the rest of society into helpless children'.[310] Britz and Ackermann employ the 'Big Brother' metaphor to describe such threats to privacy caused by state surveillance.[311] This metaphor has also been adapted to describe the threat to privacy posed by the private sector, which is often referred to as 'Little Brothers'.[312]

Solove correctly points out that the Big Brother metaphor is useful for characterising certain privacy issues arising from police search tactics, surveillance, and the disclosure of secret information; the metaphor does not, however, adequately conceptualise the privacy challenges posed by technologies capable of collecting and processing personal data without consent and enabling decisions about data subjects to be made without their meaningful participation.[313] In the US case *Olmstead v. United States* (*Olmstead*),[314] Brandeis J in his dissenting judgement states: 'Ways may someday be developed by which Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of this home.'[315] Brandeis J envisions a scenario that has since become a reality with the use of big data analytics and machine learning algorithms facilitating pervasive and potentially privacy-intrusive profiling of data subjects through the aggregation and analysis of seemingly innocuous pieces of information from various sources, public and otherwise, to create profiles or reveal sensitive personal attributes of data subjects.[316] Significantly, the privacy threat posed by the 'Little Brothers' has been gaining increasing attention as personal information becomes the asset around which companies have built veritable monopolies. It is reasonable to suggest that the threat to privacy from the private sector may be just as perilous, if not more so, than that from the government, as it is the private sector that frequently subjects individuals to decision-making without their knowledge.

---

[310] Schwartz P 'Privacy and participation: Personal information and public sector regulation in the United States' (1995) 80 *Iowa Law Review* 553 560.
[311] Britz H & Ackermann M *Information, Ethics & the Law* (2006) 48.
[312] Solove D 'Privacy and power: Computer databases and metaphors for information privacy' (2001) 53 *Stanford Law Review* 1393 1396; Britz H & Ackermann M (2006) 48.
[313] Solove D (2001) 1394–99.
[314] (1928) 277 US 438.
[315] (1928) 277 US 438 474.
[316] See 2.3.3. above.

https://uwcscholar.uwc.ac.za/home

Big data analytics has shifted focus from protecting what individuals do not wish to share, in other words maintaining secrecy, to preventing algorithms from learning about individuals' preferences and behaviours that these individuals may not even be aware of. Consequently, data protection law becomes relevant to ensure the lawful processing of personal data. The next section examines two conceptual frameworks underpinning privacy that are relevant in the South African context, namely privacy-as-secrecy and privacy-as-control.

3.2.1 Privacy-as-secrecy

During the late nineteenth century, technological innovations in printing and photography posed new privacy concerns. It was at this time that Warren and Brandeis published their article in reaction to the invasive journalistic methods facilitated by the use of new technologies.[317] This notion of privacy, understood as 'the right to be left alone' has also evolved to include an individual's right to withhold personal information from others.[318] This concept of privacy serves as the basis for US privacy laws and has also left an indelible mark on South African privacy jurisprudence.[319]

This understanding of privacy as the right to be left alone is also evident in the writings of various South African scholars and CC privacy jurisprudence. The right to be left alone informs Neethling's definition of privacy which states:

> '[A] condition of human life characterised by seclusion from the public and publicity. This condition embraces all those personal facts which the person

[317] Warren S & Brandeis L 'The right to privacy' (1890) 4 *Harvard Law Review* 193 195 explain that:

> 'Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."… The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury…'

The right to privacy may be traced to the 1890 article written by Warren and Brandeis titled 'The Right to Privacy', in which they contend that new technological inventions and business methods made the recognition of the right to privacy necessary. Prior to this article being published, the right to privacy was not recognised by any English or American Court.

[318] Warren S & Brandeis L (1890) 198.

[319] See Solove D 'Conceptualizing privacy' (2002) 90 *California Law Review* 1087 1100 for a discussion on the US discourse.

https://uwcscholar.uwc.ac.za/home

concerned has himself determined to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private.'[320]

Neethling's definition of privacy has also received judicial endorsement.[321] Similarly, Van Zyl, De Stadler and Eiselen equate the right to privacy with the right to be left alone,[322] which the CC has confirmed in various court cases.[323] To this extent, the idea of privacy in South Africa closely mirrors the understanding of privacy in the US.[324]

Despite the right to privacy being described as 'amorphous and elusive',[325] it is submitted that the South African conception of privacy is based on a secrecy paradigm. From a historical perspective, it may be argued that this could be attributed to the injustices of the past that resulted in the wanton disregard of personal privacy.[326] In a secrecy paradigm, the right to privacy may be viewed as a safeguard against government abuses aimed at addressing information practices related to the disclosure of information and surveillance by enabling individuals to conceal information. Therefore, the preservation of secrecy and concealing of information is of paramount importance.

UNIVERSITY of the
WESTERN CAPE

Moreover, the right to be left alone as understood in the South African context also draws on Warren and Brandeis' recognition of the individual's 'inviolable core'. 'Inviolate personality' is the social value protected by privacy and includes other notions too, such as individual dignity, integrity, personal autonomy and independence.[327] The CC has described this as the individuals' personal sanctum or inner sphere where their emotions, thoughts, and personal

[320] Neethling J 'The concept of privacy in South African law' (2005) 122 *SALJ* 18 19. See also Rautenbach I 'The conduct and interests protected by the right to privacy in section 14 of the Constitution' (2001) 2001 *Journal of South African Law* 115 116.

[321] *National Media Ltd and Another v Jooste* 1996 (3) SA 262 (SCA) 271B; *Bernstein and Others v Bester and Others* 1996 (2) SA 751 (CC) para 68.

[322] Van Zyl E, De Stadler E & Eiselen S 'Section 11' in Naude T & Eiselen S (eds) *Commentary on the Consumer Protection Act* (Original Service 2014) para 8.

[323] *Minister of Justice and Constitutional Development and Others v Prince and Others* 2018 (6) SA 393 (CC) para 45; *NM and Others v Smith and Others (Freedom of Expression Institute as Amicus Curiae)* 2007 (5) SA 250 (CC) para 32.

[324] See 4.3 below.

[325] *Bernstein and Others v Bester and Others* 1996 (2) SA 751 (CC) para 65; Neethling J 'The concept of privacy in South African law' (2005) 18.

[326] *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* 2021 (3) SA 246 (CC) para 26; *Gaertner and Others v Minister of Finance and Others* 2014 (1) SA 442 (CC) para 48. See also Bilchitz D 'Privacy, Surveillance and the Duties of Corporations' (2016) 1 *TSAR* 45 50–1.

[327] DeCew J 'Privacy' in Zalta E (ed) *The Stanford Encyclopedia of Philosophy* 2018 para 3.2 available at *https://plato.stanford.edu/archives/spr2018/entries/privacy/* (accessed 6 October 2020).

https://uwcscholar.uwc.ac.za/home

boundaries are considered sacrosanct.[328] This suggests that this inner realm is deserving of greater protection from external intrusions, entitling the individual to live with a degree of freedom from government and private interference. Such a conception of privacy leads to the characterisation of privacy interests as lying on spectrum, which is a cornerstone of South African privacy jurisprudence. The closer one is to the inner sphere, the more pronounced the right to privacy becomes. While the right to be left alone denotes privacy in negative terms, the conception of privacy-as-control also occupies a prominent place in South African privacy law that involves positive obligations.

3.2.2 Privacy-as-control

Individuals ought to have the ability to control the destiny of their private information and choose which personal information can be collected and used.[329] Roos expands on Neethling's definition by stating that:[330]

> '[T]he essence of an individual's interest in privacy is his or her power of self-determination over the scope of the information to be excluded from the knowledge of others. Therefore a person's right to privacy entails that he or she should have control over his or her personal information.'

UNIVERSITY of the
WESTERN CAPE

This aspect of privacy entails that a person ought to be entitled to exercise a measure of control over the processing of his personal information by others. In this regard, individuals ought to be entitled to exercise autonomy and control over their personal information and to decide what information they wish to disclose or withhold about themselves. Such decision-making ought to be free from government or private sector interference.

However, in the personal data economy, it is impossible for individuals to perform most daily activities without disclosing or sharing personal data.[331] The processing of personal information is an indispensable and most likely unavoidable part of contemporary society. This raises concerns as to whether individuals who share information do so willingly in light of the

[328] *Bernstein and Others v Bester and Others* 1996 (2) SA 751 (CC) para 67.

[329] Neethling J 'The concept of privacy in South African law' (2005) 20; *National Media Ltd and Another v Jooste* 1996 (3) SA 262 (A) 271B-272A.

[330] Roos A 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position' (2007) 124 *SALJ* 400 421–22.

[331] Mai J 'Big Data Privacy: The datafication of personal information' (2016) 32 *The Information Society* 192 193.

https://uwcscholar.uwc.ac.za/home

extensive passive collection of personal data.[332] Due to the pervasive nature of data collecting in the contemporary digital economy, individuals often have limited alternatives but to provide personal information to engage in everyday activities. Despite the many and diverse privacy concerns, many individuals continue to engage in the unprecedented sharing of personal information in the online environment.[333]

Such information is often shared consciously and willingly for a variety of reasons, including shopping, email and communication, paying taxes, entertainment and social networking sites.[334] Bergelson states, with merit, that the right to be left alone is less relevant in the personal data economy than being in control of the distribution and use of personal information by others.[335] This can be attributed to widespread data gathering practices due to the fact that it is impossible to engage in daily life without some personal data being shared because everyone makes use of technology at some point. To not do so would mean that a person must completely sever all ties and isolate themselves from society, which is not practical nor realistic. Therefore, information privacy concerns arising from individuals who willingly disclose their personal data to others cannot be satisfactorily addressed by the secrecy paradigm.[336]

UNIVERSITY of the
WESTERN CAPE

Consequently, the right to privacy has shifted from an expectation of 'the right to be left alone' to a desire to control information as a result of intrusive technologies and sophisticated data collection techniques.[337] Therefore, the dominant paradigm in an online environment conceives of privacy as an individual's right to control the use of personal information.[338] The privacy-as-control paradigm aims to enhance freedom and autonomy by affording individuals discretion as to what information they share and how their personal data is used.[339] The autonomy principle places the individual at the centre of decision-making about personal

[332] See 2.3.3 and 2.3.4 above for a discussion on compromising individual autonomy. Undermining autonomy impugns the dignity of the individuals, treats them as objects, and disregards their feelings as to how their personal information ought to be used and processed.

[333] Roos A 'Privacy in the Facebook Era: A South African Legal Perspective' (2012) 129 *SALJ* 375 392–94; Bandara R, Fernando M & Akter S 'The Privacy Paradox in the Data-Driven Marketplace: The Role of Knowledge Deficiency and Psychological Distance' (2017) 121 *Procedia Computer Science* 562 563.

[334] Solove D 'Conceptualizing privacy' (2002) 90 *California Law Review* 1087 1152; SALRC (2009) para 1.2.9; Mai J (2016) 192–93.

[335] Bergelson V 'It's Personal But Is It Mine? Toward Property Rights in Personal Information' (2003) 37 *University of California Davis Law Review* 379 401.

[336] Bergelson V (2003) 401.

[337] Alibeigi A, Munir A & Ershadul Karim M 'Right to privacy, a complicated concept to review' (2019) *Library Philosophy and Practice* 1 19.

[338] Schwartz P 'Internet privacy and the state' (1999) 32 *Connecticut Law Review* 815 820.

[339] Lazaro C & Le Métayer D 'The Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12 SCRIPTed 3 4; Bergelson V (2003) 402.

https://uwcscholar.uwc.ac.za/home

information use.[340] This paradigm forms the foundation of most data protection models.[341] As such, POPIA establishes principles for data processing in a manner that promotes the dignity of individuals and provides a clear framework for how an individual's personal information ought to be collected, processed, and shared.[342] By granting individuals certain rights over their personal data and imposing restrictions on its lawful processing, data protection regimes aim to balance information asymmetry.[343] Control is achieved principally through the informed consent mechanism, which allows individuals to evaluate options deliberately and then decide whether to give or withhold consent.[344]

Control presupposes the right of individuals to know what information about themselves is collected, to determine what information should be made available to others, and to access and update their personal information when necessary.[345] The control paradigm involves the ability of a person to ensure that personal information is used for the purpose that is desired.[346] However, a control paradigm is burdened with limitations in an online environment. A scenario involving an exchange of personal data for goods or services is fraught with privacy challenges for the data subject. Regulating privacy by requiring that personal information be collected directly from a data subject and for a specific purpose only is rendered largely meaningless in the big data environment. In the context of the IoT, passive data collection by devices and things is now the predominant method of collecting personal information, which largely eliminates the requirement for consent.[347] Moreover, data subjects are generally uninformed about the ways that their personal information is collected and how it is used.[348] Individuals have limited control and protection under current data protection regulations against data mining and predictive analysis that leverages their personal data to make conclusions that may jeopardise their privacy and reputation.[349]

---

[340] Schwartz P (1999) 820.

[341] Roos A 'Core principles of data protection law' (2006) 130; Recital 7, GDPR.

[342] The GDPR provides a similar data processing framework for the EU.

[343] Rouvroy A & Poullet Y 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Gutwirth S et al (eds) *Reinventing Data Protection?* (2009) 69; Jerome J 'Big Data: Catalyst for a Privacy Conversation' (2014) 48 *Indiana Law Review* 213 228–30.

[344] Nissenbaum H 'A Contextual Approach to Privacy Online' (2011) 140 *Daedalus* 32 34.

[345] Lazaro C & Le Métayer D (2015) 8.

[346] Solove D (2002) 1108.

[347] See 2.3.2 above.

[348] Allen A 'Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm' (2000) 32 *Connecticut Law Review* 861 869–70.

[349] Cachalia F & Klaaren J (2021) 11.

https://uwcscholar.uwc.ac.za/home

3.3 THE RIGHT TO THE PROTECTION OF PERSONAL INFORMATION

3.3.1 Common law protection

Neethling's definition of privacy provides an instructive point of departure.[350] Implicit in this definition is the individual's right to control his personal information and to decide with whom information ought to be shared.[351] For information to be private, the individual must actively express the intention or desire for it to be so;[352] this means that no information is inherently private. It follows that someone's knowledge of true facts about an individual obtained by intrusion or disclosure, contrary to the will of the individual, constitutes an infringement of privacy.[353]

Based on the foregoing, it needs to be established what constitutes 'private' in relation to personal facts. According to the definition, individuals decide what constitutes private facts. Private information is subjective and relies on the individual's personal perspective, but its protection is dependent on seclusion from the public. This conception of privacy conforms to the secrecy paradigm discussed above.[354] Privacy subsists to the extent that such information remains secret from the public. This does not, however, mean that the individual cannot disclose such information to others. When an individual discloses such information in confidence to others, it remains secret and remains protected. In other words, privacy is aimed at concealing information from others who are not entitled to receive such information. Information so disclosed implies that those with whom it was shared are identifiable by the individual, and therefore they cannot be considered to be part of the public. This conception of privacy, however, faces difficulties given modern data practices. There are 'millions of little pieces of personal information or data' that are processed and used for purposes unbeknown to the data subject.[355] In an online environment, it is impossible to maintain secrecy or seclusion without leaving a 'trail or residue'.[356] Engaging in online activities leaves data trails and digital

[350] See 3.2.1 above.

[351] Naude A & Papadopoulos S 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments (1)' (2016) 79 *Journal of Contemporary Roman-Dutch Law* 51 53; SALRC (2009) para 1.2.1.

[352] SALRC (2009) para 2.2.4.

[353] Roos A (2006) 105–6; *Financial Mail (Pty) Ltd and Others v Sage Holdings Ltd and Another* 1993 (2) SA 451 (A) 462–63.

[354] See 3.2.1 above.

[355] Roos A (2007) 401.

[356] Solove D (2004) 8.

https://uwcscholar.uwc.ac.za/home

footprints, making it possible to generate information about the lives and activities of Internet users.[357] Therefore, there is no need for an intrusion into the private sphere of a person in order to invade privacy.[358]

The definition further provides that the will of the individual is an essential factor in determining whether information is private or not. If the will for privacy is absent, then a person is not inclined towards safeguarding privacy.[359] Again, this stems from an understanding of privacy conceived as the right to be left alone. The right to be left alone places a heavy reliance on the public/private dichotomy in determining whether a legitimate expectation of privacy exists. Accordingly, privacy protection extends 'to ordinary or reasonable sensibilities and not to hypersensitivities.[360] This means that privacy extends only to a subject expectation of privacy of the individual that society considers objectively reasonable. This conception of privacy has been endorsed by the CC and is discussed further in the next section. Such a notion of privacy is problematic in a big data context because of the willingness of individuals to trade their personal data in exchange for benefits. Applying Neethling's definition to such a scenario would result in these individuals being deprived of the right to privacy. It is submitted that individuals would still harbour an expectation of privacy despite contemporary data practices. However, a privacy approach centred on secrecy is unlikely to offer individuals the necessary protection.

Under the common law, when an individual's privacy rights are infringed through the unlawful processing of personal information, the aggrieved party can rely on the law of delict for a remedy such as the actio iniuriarum for non-patrimonial loss for the injury caused to another resulting from the wrongful and intentional processing of personal information.[361] This is so because the common law has recognised the right to privacy as an independent personality right.[362] The actio iniuriarum has the object of effecting retribution for the injustice sustained by the plaintiff by compelling a defendant to compensate the plaintiff for injury to his

[357] Buchanan T et al 'Development of measures of online privacy concern and protection for use on the Internet' (2007) 58 *Journal of the American Society for Information Science and Technology* 157 157; Schwartz P (2009) 815.
[358] See 2.3.2 above.
[359] SALRC (2009) para 2.2.4.
[360] McQuoid-Mason D 'Chapter 38: Privacy' in Woolman S & Bishop M (eds) *Constitutional Law of South Africa* 2 ed (Revision Service 6) 3; *National Media Ltd and Another v Jooste* 1996 (3) SA 262 (A) 271.
[361] Roos A (2007) 423.
[362] *O' Keeffe v Argus Printing and Publishing Co Ltd* 1954 (3) SA 244 (C) 248F–48H.

https://uwcscholar.uwc.ac.za/home

personality.[363] The boni mores principle is used in determining whether conduct was offensive to the prevailing mores and adversely affected the personality interests of another, such as the right to privacy.[364] Despite common law remedies being useful in determining whether or not processing of personal information has taken place lawfully, they provide only limited data protection.[365]

Roos states, correctly in my view, that traditional delictual principles do not provide an individual with active control over the personal information that is being processed.[366] This is because delictual principles are generally backward looking. Delictual principles provide only protection against already committed wrongs and do not prevent or impose restrictions on the unlawful processing of personal information. Active control implies that individuals have the right to take specific actions regarding the processing of their personal information. Moreover, if an individual initiates a reasonable and lawful action, the other party wishing to process such information has a corresponding duty to cooperate.

Neethling points out that it is highly unlikely that courts will apply traditional principles 'often or extensively enough in the near future' to warrant the reliance on the courts to develop the common law for the protection of personal information,[367] notwithstanding the obligation of the courts to develop the common law in accordance with the spirit, objects and purport of the Bill of Rights.[368] It is submitted that traditional principles cannot offer adequate data protection for several reasons. First, the common law has been developed over centuries with reference to the boni mores, moral standards and the common notion of what is right and fair. Since the technologies discussed in chapter two are relatively recent developments, they did not exist as the common law developed. Secondly, while it is reasonable to state that the common law adapts to technological change and is therefore flexible, such change does not occur quickly enough to offer any meaningful protection.[369] The difficulty of the common law adapting is further highlighted if one considers that technological advancements and the concomitant

[363] Neethling J & Potgieter J *Law of Delict* 8 ed (2021) 290 301–2.

[364] Neethling J 'Grondslag vir die erkenning van 'n selfstandige persoonlikheidsreg op privaatheid in die Suid-Afrikaanse reg' (1976) 39 *THRHR* 121 125.

[365] Roos A (2008) 92.

[366] Roos A (2007) 423. Similar reservations have been expressed in the US context. See 4.5 below.

[367] Neethling J (2012) 245.

[368] Neethling J, Potgieter J & Visser P *Neethling's Law of Personality* 2 ed (2005) 55.

[369] Cachalia F & Klaaren J (2021) 8 state that privacy as solely a common law or delictual matter is typical of South Africa's pre-1994 legal system and is generally characterised by its inability to respond to technological change.

https://uwcscholar.uwc.ac.za/home

challenges often outpace legislation enacted to address specific areas of law, which is evident in the case of personal information.[370] Thirdly, the common law cannot offer sufficient protection and safeguards that other countries may demand in relation to the transfer of personal data. Fourthly, if given the option to institute legal action based on the common law or statutory protection, individuals are unlikely to choose the common law.[371]

3.3.2. Constitutional protection

As stated previously, Neethling's definition of privacy has been judicially endorsed and applied in several CC cases.[372] In terms of the constitutional right to privacy, individuals have the ability to decide which information they want to make public, as long as their expectation of privacy is reasonable.[373] The right to informational privacy within the broader protection of the right to privacy was recognised in *Mistry v Interim Medical and Dental Council of South Africa*.[374] Privacy extends to those aspects of a person's life in regard to which a legitimate expectation of privacy can be harboured.[375] In this regard, the CC draws on the US experience in *Katz v United States,*[376] in which the US Supreme Court constructs a test to determine the existence of a 'reasonable expectation of privacy'.[377]

Viewing privacy as the right to be left alone enables individuals to maintain a personal or intimate space that is free from outside intrusion. A legitimate expectation of privacy can therefore be reasonably assumed in the 'inner sanctum of a person's life' or the 'truly personal realm'.[378] A 'truly personal realm' represents the most personal aspects of a person's existence, such as family life, sexual preference, and home environment.[379] In determining what

---

[370] See the reference to the 'pacing problem' in 3.1 above.

[371] Swales L 'The Protection of Personal Information Act 4 of 2013 in the Context of Health Research: Enabler of Privacy Rights or Roadblock?' (2022) 25 *PELJ* 1 3.

[372] See 3.2.1 above.

[373] *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd and Others: In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* 2001 (1) SA 545 (CC) para 16.

[374] *Mistry v Interim Medical and Dental Council of South Africa and Others* 1998 (4) SA 1127 (CC) 1155G–1156A.

[375] Roos A (2008) 93; *Bernstein and Others v Bester and Others* 1996 (2) SA 751 (CC) paras 74–5.

[376] (1967) 389 US 347.

[377] (1967) 389 US 347 361.

[378] *Bernstein and Others v Bester and Others* 1996 (2) SA 751 (CC) para 67.

[379] *Bernstein and Others v Bester and Others* 1996 (2) SA 751 (CC) para 67; *National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others* 1999 (1) SA 6 (CC) para 31; Neethling J 'The concept of privacy in South African law' (2005) 20; *Investigating Directorate: Serious Economic Offences v*

https://uwcscholar.uwc.ac.za/home

constitutes a legitimate expectation, it must be shown that a subjective expectation of privacy that society considers objectively reasonable exists.[380]

In *Mistry v Interim Medical and Dental Council of South Africa*,[381] the CC described the content of the right to privacy as a 'continuum of privacy rights which may be regarded as starting with a wholly inviolable inner self, moving to a relatively impervious sanctum of the home and personal life and ending in a public realm where privacy would only remotely be implicated'.[382] Privacy becomes more intense the closer it is to the intimate personal sphere and less intense as it moves towards the periphery.[383] However, technologies are an integral part of modern-day living, and 'we conceive of them often as a central part of our "private world" through which we conduct our "private" business'.[384] In light of these technological changes, Langa DP in *Hyundai* submits, correctly in my view, that the right to privacy does not relate solely to an individual within his intimate sphere, and therefore the statements in *Bernstein* should not be construed as an absence of the right to privacy when persons socially interact with others. [385] People retain the right to be left alone by the state even when they are in their offices, cars or on their mobile telephones.[386] This means that the inviolable core is located at the far end of the spectrum and that venturing into public spaces, which means moving in the opposite direction, weakens privacy protection without necessarily removing it entirely.

Therefore, a conception of privacy as lying on a continuum is based on an understanding and articulation of the right to privacy as the right to be left alone, free from interference by the government or any other party.[387] Privacy is infringed when 'one's hidden world' is revealed,

---

Hyundai Motor Distributors (Pty) Ltd and Others: In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others 2001 (1) SA 545 (CC) para 16.

[380] McQuoid-Mason D 'Chapter 38: Privacy' in Woolman S & Bishop M (eds) *Constitutional Law of South Africa* vol Revision Service 6 (2 ed) 30.

[381] *Mistry v Interim Medical and Dental Council of South Africa and Others* 1998 (4) SA 1127 (CC).

[382] 1998 (4) SA 1127 (CC) para 27.

[383] De Vos P & Freedman W (eds) *South African Constitutional Law in Context* (2014) 463; *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd and Others: In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* 2001 (1) SA 545 (CC) para 16 para 18.

[384] Bilchitz D (2016) 45.

[385] *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd and Others: In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* 2001 (1) SA 545 (CC) para 16.

[386] 2001 (1) SA 545 (CC) para 16.

[387] Mia N 'The Problems with Prince: A Critical Analysis of Minister of Justice and Constitutional Development v Prince' (2020) 10 *Constitutional Court Review* 401 414; *NM and Others v Smith and Others (Freedom of Expression Institute as Amicus Curiae)* 2007 (5) SA 250 (CC) para 32; *Minister of Justice and Constitutional Development and Others v Prince and Others* (2018) 6 SA 393 (CC) para 45; *Amabhungane Centre for*

https://uwcscholar.uwc.ac.za/home

either through surveillance or the disclosure of concealed information that results in harm to the individual, including inhibition, self-censorship, embarrassment, and reputational damage.[388] This understanding places a heavy reliance on the public/private dichotomy in determining whether a legitimate expectation of privacy exists.

In view of the personal data economy, it is submitted that a reappraisal of the reliance on the inviolable core is necessary. *Bernstein*, which is regarded as the seminal case dealing with privacy in South Africa, was decided under the Interim Constitution at a time when many of the technological developments and privacy concerns outlined in chapter two did not exist. Bernstein's conception of privacy raises questions about whether a privacy continuum based on an inviolable core is relevant given contemporary data practices. Moreover, it raises further questions about whether the right to privacy should encompass these data practices. It is submitted that such a conception of privacy becomes less relevant for several reasons, and the reasoning of Langa DP in Hyundai provides support for such an argument. His opinion assumes even greater significance in view of the technological developments discussed in chapter two. At the time, Langa DP recognised that privacy cannot be limited solely to the intimate sphere of an individual's life. If one puts this into perspective now, communal relationships are increasingly important for social and business reasons. People spend a lot of time online for various reasons.[389] Aside from the social media phenomenon, government and the private sector have all adopted digital solutions to deliver services. As a result, people find themselves compelled to use these digital services for their everyday activities, which require them to share or disclose personal information. In this sense, individuals cannot freely exercise a choice to be left alone.

Privacy, defined as the right to be left alone, posits that if information is no longer secret, it ceases to be private, a notion that is not sustainable in the age of big data.[390] Schwartz states: 'The proper social response to information privacy issues cannot be to maximise secrecy about individuals and their pursuits.'[391] In an online environment, secrecy means that an individual desiring privacy must disconnect from all activities to isolate himself from the world, which in

Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others 2021 (3) SA 246 (CC) para 2; Mashinini N 'The Processing of Personal Information Using Remotely Piloted Aircraft Systems in South Africa' (2020) *De Jure Law Journal* 140 145.

[388] Solove D (2004) 8; *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* 2021 (3) SA 246 para 24.

[389] See 3.2.2 above.

[390] Solove D (2004) 8.

[391] Schwartz P (1999) 834.

https://uwcscholar.uwc.ac.za/home

today's society is not practical given the reliance on technology and the pervasiveness thereof in modern life.[392] Lukács writes:[393]

> 'Nowadays we live in the era of the information society, which has a huge impact on our lives… [T]he private sphere of someone becomes more open, as the new developments make more intrusion into it, more and more aspects of private life can be reached or touched through technologies.'

As the private or intimate sphere becomes more exposed, the question that ought to be asked is whether the understanding of privacy that is premised on considerations such as space, secrecy and seclusion, which implicates the inner sanctum as articulated by *Bernstein* and other CC cases,[394] is still relevant. For example, an individual would conventionally attain privacy by retreating to a room and closing the door, thereby avoiding unwanted intrusions and disturbances.[395]

In *Minister of Justice and Constitutional Development and Others v Prince*,[396] the CC held the right to privacy extends beyond the home,[397] and in so doing ignoring the long-standing spatial considerations. According to the CC in *Prince*, privacy does not mean being confined to one's home. Mia is critical of the judgement to extend the scope of privacy beyond the home without providing a clear justification for doing so and suggests that the CC could have drawn on the jurisprudence between privacy rights and protection of the autonomy of the individual as a basis for its decision.[398] I agree with Mia's criticism of *Prince* to the extent that it suggests the conception of privacy as relating to autonomy or control would offer greater elucidation for extending privacy beyond the home than an understanding of privacy as the right to be left alone. The *Prince* decision is significant as it brings into question whether a conception of

---

[392] Papadopoulos S 'Revisiting the public disclosure of private facts in cyberworld' (2009) *Obiter* 30 38.

[393] Lukács A *What Is Privacy? The History and Definition of Privacy* (2016) 256 261.

[394] *Case and Another v Minister of Safety and Security and Others; Curtis v Minister of Safety and Security and Others* 1996 (3) SA 617 (CC) para 91; *Mistry v Interim Medical and Dental Council of South Africa and Others* 1998 (4) SA 1127 (CC) para 27; *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd and Others: In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* 2001 (1) SA 545 (CC) para 16; *Gaertner and Others v Minister of Finance and Others* 2014 (1) SA 442 (CC) para 49; *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* 2021 (3) SA 246 (CC) para 24.

[395] Könings B & Schaub F *Territorial Privacy in Ubiquitous Computing* (2011) 105.

[396] 2018 (6) SA 393 (CC). The matter concerned the constitutionality of the prohibition and criminalisation of the private use, possession and cultivation of cannabis by adult persons and whether such prohibition constituted an infringement of privacy.

[397] 2018 (6) SA 393 (CC) para 100.

[398] Mia N (2020) 413–17.

https://uwcscholar.uwc.ac.za/home

privacy with an emphasis on physical spaces that seek to maximise seclusion and secrecy is still relevant in today's online or virtual environment. Whereas the physical boundaries of a room would have marked the boundaries of an individual's sphere of privacy, this is no longer the case.[399] Online communication is an integral part of interpersonal relationships, so the perception of privacy and the reliance on spatial factors ought to be reconsidered.

In *National Coalition*, Sachs J correctly asserted in his concurring judgement that the right to privacy afforded to individuals relates to people, not places.[400] Even though technologies can be used in the most intimate of spaces, thereby shifting boundaries as to what was traditionally considered public or private, secret and intimate, this should not in any way mean that individuals are no longer entitled to their privacy. Given the important role that technology plays in everyday life and its influence on how personal information is collected, processed and shared, it is argued that there is no reason as to why the level of privacy protection ought to attenuate in instances where such information is used outside of the personal or intimate sphere. As such, any infringement of privacy ought to result in a breach along the entire privacy spectrum.

Despite the existence of a constitutional legal framework that protects informational privacy, data protection under the Constitution is handicapped by the application of ordinary private law principles, as with common law.[401] Purtova supports the idea that data protection laws need to provide data subjects with positive rights to prevent the unlawful processing of personal information, since negative rights are only about remedying wrongs that have already been done.[402] Roos correctly contends that the state has a constitutional obligation to enact legislation to provide effective informational privacy protection in light of the limitations of ordinary private law principles.[403]

UNIVERSITY of the
WESTERN CAPE

[399] Könings B & Schaub F *Territorial Privacy in Ubiquitous Computing* (2011) 105.

[400] *National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others* 1999 (1) SA 6 (CC) para 116.

[401] Roos A (2008) 93.

[402] Purtova N (2009) 512. See also Roos A (2008) 93.

[403] Roos A (2007) 423. Roos explains that it is the task of the legislature and not the judiciary to introduce new legislation. See also *Carmichele v Minister of State and Security and Another (Centre for Applied Legal Studies Intervening)* 2001 (4) SA 938 (CC) para 36.

https://uwcscholar.uwc.ac.za/home

3.3.3 Statutory protection

The purpose of POPIA is to give effect to the constitutional right to privacy by regulating the collection and processing of personal information.[404] The right to privacy under POPIA is not absolute and must be balanced against other rights such as the right of access to information and the free flow of information within South Africa and across international borders.[405] POPIA has been designed to uphold the constitutional right to privacy by ensuring that personal information is processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.[406] In this regard, POPIA aims to promote individuals' dignity, autonomy, and control in relation to the processing of their personal information.

POPIA provides for eight conditions that must be satisfied for the lawful processing of information:[407]

- Accountability provides that the onus is on the responsible party to establish an environment conducive to the lawful processing of personal information;[408]

- processing limitation provides that personal information must be processed in a lawful and reasonable manner that avoids infringing on the privacy of the data subject. The personal information must be collected directly from the data subject;

- purpose specification requires that personal information must be collected for specific, explicitly defined, and lawful purposes;

- further processing limitation provides that new processing activities must be compatible with the purpose for which the information was collected initially;

- information quality requires reasonable steps to be taken to ensure that personal information that has been collected is complete, accurate, and not misleading;

[404] Section 2(a), POPIA.
[405] Section 2(a), POPIA.
[406] Section 9, POPIA.
[407] Sections 8–25, POPIA.
[408] Section 1 of POPIA defines responsible party as any ‘public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information’.

UNIVERSITY of the WESTERN CAPE
https://uwcscholar.uwc.ac.za/home

- openness provides that data subjects must know that their personal information is being collected and the purpose for which it is being collected;

- security safeguards require appropriate security measures be implemented to protect the integrity and confidentiality of personal information; and

- data subject participation provides that data subjects must have access to their personal information to update it or request corrections or deletions of information.

Meeting these eight conditions presumes the resulting processing is lawful, ensuring an adequate level of data protection and upholding the right to privacy. Effective data protection requires that an individual be able to exercise a measure of active control over his personal information, which can only be realised through data protection legislation.[409] The data subject may under certain circumstances, withdraw consent,[410] request destruction or deletion (erasure) of personal information,[411] receive information about the personal information being collected and the source from which it is collected,[412] object, on limited grounds, to the processing of personal information,[413] obtain access to personal information about him that is held by others,[414] obtain restriction of processing where the accuracy of the personal information is being contested or the processing is deemed unlawful,[415] and request rectification of incorrect or inaccurate personal information.[416] It is significant to note that POPIA and the GDPR grant data subjects almost identical data protection rights, which serves to promote the dignity of the data subjects.[417]

Although the informational privacy of the data subject is an integral part of data protection, the objective of POPIA is to regulate the flow of information. In other words, the aim is to strike a balance between privacy and the free flow of information. This conception of privacy is more aligned with a privacy-as-control paradigm and represents a shift in understanding privacy as related to secrecy and seclusion to an understanding that revolves around the control of

[409] SALRC (2009) para 2.4.4.
[410] Section 11(2)(b), POPIA.
[411] Section 24, POPIA.
[412] Section 18, POPIA.
[413] Section 11, POPIA.
[414] Section 23, POPIA.
[415] Section 14(6), POPIA.
[416] Section 24, POPIA.
[417] See 5.4.1 below.

https://uwcscholar.uwc.ac.za/home

personal information.[418] This is so because a notion of privacy derived from Neethling's definition of privacy is not open to the idea of a free flow of information. The SALRC Report makes it clear that economic and commercial reasons were key motivating factors in introducing data protection legislation like POPIA to facilitate the flow of information.[419] Therefore, it may be argued that POPIA can be seen as a legislative effort to recognise and reflect the economic significance of personal information in commerce. Significantly, data protection like POPIA does not treat personal information as a commodity, nor does it preclude the possibility. This is an important which will be discussed further in the chapters that follow.

However, the SALRC, in recognising the need for such legislation, proceeds to state that 'a proper balance has to be found between the different competing interests, namely, an open and accountable society on the one hand, and the right to be left alone on the other'.[420] I agree with the statement by the SALRC insofar as a balance must be struck between competing interests. This is so because no right, including the right to privacy, is absolute.[421] However, I do not agree that achieving such a balance is possible if one of the competing interests is the right to be left alone. A conception of privacy based on the right to be left alone, as articulated in *Bernstein* and read in conjunction with the dictum of Langa DP in *Hyundai*, suggests that a proper balance cannot be achieved because a free flow of information envisages a more public space that is far removed from the inviolable core meaning that privacy protection is attenuated.[422] It is doubtful that, in such a case, POPIA would be able to achieve its objectives since the free flow of information is diametrically opposed to the right to be left alone. This raises the question whether data protection ought to be accommodated under the constitutional right to privacy. This will be discussed in the next section.

3.4 RELATIONSHIP BETWEEN PRIVACY AND DATA PROTECTION

To speak about the right to constitutional privacy in South Africa is essentially discussing 'dignity, equality, and freedom'. In *Khumalo v Holomisa*,[423] O'Regan J opines that 'there is a

[418] See 3.2.2 above.

[419] SALRC (2009) 1.2.8–1.2.9.

[420] SALRC (2009) 1.2.8. This is also the case with other jurisdictions, such as the US and EU, where competing interests must be weighed against each other. For example, as will be discussed in the chapter four, the right to privacy in the US often comes into conflict with first amendment rights.

[421] *Bernstein and Others v Bester and Others* 1996 (2) SA 751 (CC) para 67.

[422] See 3.3.2 above.

[423] 2002 (5) SA 401 (CC).

https://uwcscholar.uwc.ac.za/home

close link between human dignity and privacy'.[424] These rights are enshrined in the Constitution as two distinct rights,[425] and although they are not completely synonymous, they largely overlap in their application. Therefore, whenever the constitutional right to privacy is implicated, it will often involve a consideration of other values including dignity. In this regard, the right to privacy serves to foster human dignity.[426] In *S v Makwanyane*,[427] the CC held that the right to life and dignity are values of the highest order under the Constitution.[428] Unsurprisingly, dignity informs the content of most other rights, including the right to privacy.[429] Therefore, when interpreting the constitutional right to privacy, it ought to be done in a manner that gives a broad scope of application to the values of dignity, equality and freedom.

In the introduction to this chapter, it was stated that issues stemming from the processing of personal information are typically classified as privacy matters. This is indeed true in the South African context as POPIA was designed by the legislature to 'give effect to the constitutional right to privacy'.[430] Therefore, it can be deduced that POPIA's data protection framework aims to promote the dignity and autonomy of data subjects. Following this, it is reasonable to argue that any unlawful processing of personal information may implicate the right to privacy of the data subject. The question that arises is whether data protection is simply privacy under another guise.

Roos opines that data protection is an aspect of privacy and therefore a fundamental right entrenched in s 14 of the Constitution.[431] On the other hand, Donnelly states that the Constitution protects the right to privacy, not the right to data protection.[432] Despite the seemingly differing perspectives, both views suggest areas of overlap and differences. The EU,

[424] 2002 (5) SA 401 (CC) para 27.

[425] Section 10 of the Constitution deals with the right to human dignity and s 14 deals with the right to privacy.

[426] *Khumalo and Others v Holomisa* 2002 (5) SA 401 (CC) para 27.

[427] 1995 (3) SA 391 (CC).

[428] 1995 (3) SA 391 (CC) para 111.

[429] *Dawood and Another v Minister of Home Affairs and Others; Shalabi and Another v Minister of Home Affairs and Others; Thomas and Another v Minister of Home Affairs and Others* 2000 (3) SA 936 (CC) para 35. See also *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* 2021 (3) SA 246 (CC) para 28.

[430] Section 2, Constitution.

[431] Roos A 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position' (2007) 124 *SALJ* 400 402–3.

[432] Donnelly D *Privacy by (Re)Design: A Comparative Study of the Protection of Personal Information in the Mobile Applications Ecosystem under United States, European Union and South African Law* (unpublished LLD thesis, University of KwaZulu-Natal, 2020) 10–1.

https://uwcscholar.uwc.ac.za/home

in contrast to South Africa, recognises the right to privacy and the protection of personal data as two distinct rights.[433] Such a distinction is not recognised in South Africa as the Constitution considers data protection a subset of the right to privacy.[434] However, Neethling points out, in his criticism of *Bernstein*, that the concept of privacy formulated in that case is too narrow and fails to account for the relatively trivial or insignificant information that may be collected and processed.[435] This is precisely the crux of the matter. In chapter two, it was demonstrated how technologies can collect trivial bits of information to analyse and draw inferences that are potentially privacy invasive. It is submitted that a notion of privacy based on the right to be left alone cannot offer adequate protection in such instances because the information so collected may not be personal or sensitive enough to warrant protection as is demonstrated in the following case.

In *Amabhungane Centre for Investigative Journalism NPC v Minister of Justice (Amabhungane)*,[436] the CC considered the impact of surveillance technologies on the right to privacy. In this regard, the CC states:[437]

> 'Today technology enables law enforcement agencies to not only physically – as opposed to electronically – invade the "intimate personal sphere" of people's lives, but also to maintain and cement its presence there, continuously gathering, retaining and – where deemed necessary – using information.'

The quote by the CC reinforces the South African conception of privacy as the right to solitude. As such, the emphasis is on maintaining secrecy or concealing information from interference from the government and others. *Amabhungane* concerns the unlawful interception of private communications of individuals.[438] Communications may include verbal conversations, emails and cellular exchanges that are transmitted a through a postal service or a telecommunication network.[439] However, those communications are protected only to the extent that a legitimate expectation of privacy can be harboured. In other words, the interception of trivial information does not constitute a privacy infringement because an individual cannot have a legitimate

[433] See 5.3.1 below.
[434] *Mistry v Interim Medical and Dental Council of South Africa and Others* 1998 (4) SA 1127 (CC) 1155G–1156A.
[435] Neethling J 'The Concept of Privacy in South African Law' (2005) 20.
[436] *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* 2021 (3) SA 246 (CC).
[437] 2021 (3) SA 246 (CC) para 1.
[438] 2021 (3) SA 246 (CC) para 2.
[439] 2021 (3) SA 246 (CC) para 7.

https://uwcscholar.uwc.ac.za/home

expectation of privacy with respect to such information, but a privacy breach may result if the information is part of his private communications. A further example to distinguish between privacy and data protection would be if someone were to compile a data record by obtaining bits of personal information associated with an individual that is available publicly, such as gender, sexual orientation, marital status or religion. These types of information are defined as personal information under POPIA.[440] A compilation of such a data record constitutes processing under POPIA but does not necessarily imply an intrusion into the intimate personal sphere of the person to whom it is linked. It is submitted that this is so even if the processing is carried out unlawfully, for example, without the consent of the individual. Privacy is only infringed when the data record is used in a manner that reveals information about an individual that they wish to keep private. These privacy concerns typically arise when big data analytics and profiling are used.[441] Therefore, it is argued that personal information does not necessarily equate to information that forms part of the intimate personal sphere.

Several scholars support such an argument. Cuijpers opines that data protection and privacy are not the same.[442] Lynskey argues that data protection offers individuals a broader range of protection than the right to privacy in the context of data processing.[443] Abdulrauf and Fombad point out that '… personal data within the context of data protection does not necessarily have to be secret or even private. This fundamentally distinguishes the right to data protection from privacy'.[444] It is therefore submitted that data protection should be conceived as a right that overlaps significantly with privacy but offers distinct benefits.[445]

Such a position has been adopted in the EU, which recognises a right to both privacy and the protection of personal data.[446] It is further submitted that the overlap stems from data protection having its roots in privacy and that data protection, like privacy, seeks to protect other fundamental rights and values such as human dignity and autonomy.[447] Beyond this intersection, the right to privacy is concerned with safeguarding the person's private sphere

[440] See section 1 of POPIA.
[441] See 2.3 above.
[442] Cuipers C 'A private law approach to privacy; mandatory law obliged?' (2007) 4 *SCRIPTed* 304 312.
[443] Lynskey O *The Foundations of EU Data Protection Law* (2015) 90.
[444] Abdulrauf L & Fombad C 'Personal data protection in Nigeria: Reflections on opportunities, options and challenges to legal reforms' (2017) 38 *Liverpool Law Review* 105 111.
[445] Lynskey O 'Deconstructing data protection in the EU legal order' (2014) 63 *International and Comparative Law Quarterly* 569 582.
[446] See 5.3.1 below.
[447] Abdulrauf L & Fombad C (2017) 114.

https://uwcscholar.uwc.ac.za/home

and preventing interference by others with respect to bodily integrity, decisional privacy, and the privacy of the home, whereas data protection involves the processing of personal data by imposing conditions on others in relation to the processing of such information regardless of whether the right to privacy is implicated.[448]

This section examines the relevance of personal information insofar as it relates to the interplay between privacy and data protection. However, in the previous chapter, another dimension to the processing of personal information was raised relating to the transformative effect of such processing on the actual personal information, namely the commodification thereof.[449] The next section briefly discusses this aspect, which goes beyond privacy and data protection, and will also lay the groundwork for the discussion in the chapters that follow.

3.5 LOOKING BEYOND PRIVACY AND DATA PROTECTION

Privacy is recognised as a personality interest at common law under the concept of dignitas and is protected by the actio iniuriarum.[450] Personality rights are non-patrimonial in nature and cannot exist independently of a person, as such rights are related to his personality.[451] Moreover, personality rights exhibit the following characteristics:[452]

- they are non-transferable;
- non-heritable;
- incapable of being relinquished or attached;
- cannot prescribe; and
- come into existence and terminate on the birth and death of a human being respectively.

[448] Hildebrandt M *Law for Computer Scientists and Other Folk* (2020) 128–31.

[449] See 2.3.4.1 above.

[450] *Bernstein and Others v Bester and Others* 1996 (2) SA 751 para 68; Zimmerman R *The Law of Obligations: Roman Foundations of the Civilian Tradition* (1990) 1084; Burchell J (2009) 3; Neethling J 'The concept of privacy in South African law' (2005) 18; McQuoid-Mason D (1978) 30; *O' Keeffe v Argus Printing and Publishing Co Ltd* 1954 (3) SA 244 (C) 249D–249E.

[451] Neethling J 'Personality rights: Comparative overview' (2005) 223.

[452] Neethling J 'Personality rights: Comparative overview' (2005) 223.

https://uwcscholar.uwc.ac.za/home

From a South African perspective, privacy is recognised as an important aspect of personality and data protection, in turn, is an element of the right to privacy.[453] By parity of legal reasoning, it is submitted that data protection serves and supports a person's personality interests. Above it was mentioned that data protection protects privacy by regulating how personal data may be processed lawfully while simultaneously ensuring the free flow of information.[454] Notably, the free flow of information has resulted in personal information becoming economically valuable.[455] This has inevitably led to personal information being viewed as a commodity that can be traded or exchanged by individuals for goods or services.[456] It is submitted that POPIA appears to embrace an approach that encourages such a view.

The human rights framework of POPIA protects the right to privacy and fosters autonomy and dignity. As such, POPIA does not envisage personal information as a thing that can be traded, nor does it consider or treat personal information as a commodity or form of property. However, there are certain aspects within the POPIA data protection framework that allows for the conception of an alternative legal framework based on property. These aspects will be briefly set out below.

UNIVERSITY of the
WESTERN CAPE

First, the primary motivation for POPIA's inception was economic to facilitate the free flow of information.[457] Secondly, POPIA, perhaps inadvertently, creates a property regime that aims to allocate a property entitlement to the data subject. In this regard, the language used in POPIA seems to support such an assertion. For example, s 2(c) of POPIA states that the purpose of POPIA is to 'provide persons with rights and remedies to protect their personal information…'. The use of the word 'their' suggests that the personal information belongs to the data subject with whom it is associated.[458] Moreover, POPIA is littered with the use of possessive pronouns such as 'his, her, its' throughout. Thirdly, the consent-based rules contained in the POPIA data protection framework allow for the transferability of personal information from the data subject

[453] Batchelor B & Wazvaremhaka T 'Balancing Financial Inclusion and Data Protection in South Africa: Black Sash Trust v Minister of Social Development' (2019) 136 *SALJ* 112 119–20; Roos A (2007) 402–3; Neethling J 'Personality Rights: Comparative Overview' (2005) 234.

[454] See 3.3.3 above.

[455] Kelly R & Swaby G 'Consumer protection rights and "free" digital content' (2017) 23 *Computer and Telecommunications Law Review* 165 166.

[456] Prins C 'Property and privacy: European perspectives and the commodification of our identity' in Guibault L & Hugenholtz P (eds) *The Future of the Public Domain* (2006) 230; Bottis M & Bouchagiar G 'Personal data v. Big data: Challenges of commodification of personal data' (2018) 8 *Open Journal of Philosophy* 206 209–10; Zarsky T (2015) 164.

[457] See 3.3.3 above.

[458] See s 5(a)–(i) of POPIA.

https://uwcscholar.uwc.ac.za/home

to another person.[459] Fourthly, POPIA imposes restrictions on the use of personal information that also apply to third parties.[460] Lastly, a data subject may institute civil action for damages in the event of misuse of personal information.[461]

These elements identified above appear to support the argument that the processing of personal information cannot be viewed solely as a matter of data protection or privacy. Doing so would ignore the fact that personal information can be treated like an economic asset, giving rise to further legal implications that require consideration. This is an aspect that will be explored further in the chapters that follow.

It is important for the law to be able to adapt and react to disruptive technological advancements by reassessing current ideas and developing more suitable ones. The problems posed by technological developments have repercussions for the democratic functioning of the state. *Amabhungane* demonstrates how modern surveillance technologies might threaten democracy by allowing the state to invade an individual's private space. Moreover, the accretion of private power poses significant problems insofar as it relates to the commodification of personal information. In this sense, it is necessary for the Constitution to find application in both the public and private spheres to ensure that the values and principles enshrined in the Constitution are recognised and observed by all.

UNIVERSITY of the
WESTERN CAPE

3.6 TRANSFORMATIVE NATURE OF THE CONSTITUTION

The Constitution possesses several distinct features that could enhance its ability to respond to change and challenges brought about by technology. These features include the transformative nature of the Constitution and the principles of horizontality and subsidiarity.

3.6.1 Transformative constitutionalism

The right to privacy is a cornerstone of democracy and is recognised, in modern times, as one of the most important human rights.[462] The right to privacy provides a means to address past

[459] Section 11(1)(a), POPIA.
[460] See the conditions for lawful processing in 3.3.3 above.
[461] Section 99, POPIA.
[462] Van der Bank C 'The right to privacy – South African and comparative perspectives' (2012) 1 *European Journal of Business and Social Sciences* 77 78; *NM and Others v Smith and Others (Freedom of Expression*

https://uwcscholar.uwc.ac.za/home

injustices and reaffirm practices that are consistent with new constitutional values.[463] The development of the constitutional right to privacy embraces the notion of transformation, which aims to effect positive societal and economic change.[464] Transformation, in this sense, aspires to effect a continual evolution that requires ongoing effort to consistently improve the quality of life for people by interpreting the law in a manner that promotes, protects and fulfils the rights and freedoms as enshrined in the Constitution. In other words, the Constitution needs to remain relevant and be able to adapt to emerging challenges to meet societal needs.

Chapter two illustrated that technology advancements give rise to a myriad of new issues. Therefore, the Constitution's underlying values and ideals ought to apply in light of the challenges of contemporary society. Given that private actors pose as much of a threat to the rights of individuals as the state, it is necessary that the values enshrined in the Constitution extend to the private sector as well. Disregarding private relationships would result in the Constitution's failure to effectively protect the dignity of persons. Therefore, transformative constitutionalism will be relevant to the development of the law to cope with the challenges arising from the commodification of personal information. In this regard, s 7(2) imposes certain obligations on the state while ss 8(2) and 8(3) extends the application of the Bill of Rights to private relationships.

UNIVERSITY of the
WESTERN CAPE

3.6.2 Horizontality

Another characteristic of the transformative nature of the Constitution is the concept of horizontality. The objective of fundamental rights was originally intended to limit the misuse of state authority; nevertheless, it is now recognised that the impact on fundamental rights as a result of the private sector's expanding influence is a developing worry.[465] Zuboff labels this 'surveillance capitalism', which is the accumulation of knowledge about individuals by companies like Facebook, Amazon, and Google to predict, influence, and modify the behaviour of such individuals for commercial gain.[466] Threats to privacy are no longer limited to the

Institute as Amicus Curiae) 2007 (5) SA 250 (CC) para 133; *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* 2021 (3) SA 246 (CC) paras 26–7.

[463] *Gaertner and Others v Minister of Finance and Others* 2014 (1) SA 442 (CC) para 48.

[464] Langa P 'Transformative constitutionalism' (2006) 17 *Stellenbosch Law Review* 351 351–54; *S v Makwanyane and Another* 1995 (3) SA 391 (CC) para 252.

[465] Bilchitz D 'Privacy, surveillance and the duties of corporations' (2016) 1 *TSAR* 45 47–8.

[466] Zuboff S *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (2019) 16–8. Zuboff states 'ownership of the new means of behavioural modification eclipses ownership of the means of production as the fountainhead of capitalist wealth and power in the twenty-first century'.

https://uwcscholar.uwc.ac.za/home

exercise of power by the state but include harms resulting from the power wielded by the private sector.[467]

The Bill of Rights, as set out in chapter two of the Constitution, contains the entrenched fundamental rights that are binding on the executive, the legislature, the organs of state, the judiciary, and all persons (natural and juristic).[468] Fundamental rights may be limited in terms of the s 36 limitation clause of the Constitution, and any such limitation, contained in a law of general application, must, to pass muster, be reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom.[469] The right to privacy is not absolute. In *Bernstein and Others v Bester and Others*,[470] the Court held '[t]he truism that no right is to be considered absolute implies that from the outset of interpretation each right is always already limited by every other right accruing to another citizen'.[471] The right to privacy ought to be weighed against opposing rights and interests, such as, for example, the right to freedom of expression and access to information as provided for in terms of s 16 and 32 of the Constitution respectively.[472] This normative enquiry is required by s 39 of the Constitution, which provides that the Bill of Rights must be interpreted in a manner that 'promotes the values which underlie an open and democratic society based on human dignity, equality and freedom'.[473]

In *Du Plessis v De Klerk*,[474] the CC held that entrenched fundamental rights were irrelevant to private litigation to the extent that no government conduct or legislation was relied upon by either party to the litigation.[475] Mupangavanhu criticises the decision of the court as this would imply that fundamental rights cannot be invoked by one private party against another.[476] In

[467] Cachalia F & Klaaren J (2021) 13.

[468] Sections 8(1), 8(2) and (4), the Constitution. In terms of s 8(4), juristic persons are entitled to the Bill of Rights 'to the extent required by the nature of the rights and the nature of that juristic person'. In *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd and Others: In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* 2001 (1) SA 545 (CC) para 18, the CC held that juristic persons therefore do enjoy the right to privacy, although not to the same extent as natural persons.

[469] Section 36, Constitution; Neethling J 'Die Reg Op Privaatheid En Outonomie Prince v Minister of Justice and Constitutional Development 2017 4 SA 299 (WCC); [2017] 2 All SA 864 (WCC)' (2018) 15 *LitNet Akademies* 486 492; SALRC (2009) para 1.2.7.

[470] 1996 (2) SA 751 (CC).

[471] 1996 (2) SA 751 (CC) para 67.

[472] *Arena Holdings (Pty) Ltd t/a Financial Mail and Others v South African Revenue Service and Others* 2023 (8) BCLR 905 (CC) paras 129–46. See also SALRC (2009) para 2.2.21.

[473] Section 39(1)(a), Constitution.

[474] 1996 (3) SA 850 (CC).

[475] 1996 (3) SA 850 (CC) para 49.

[476] Mupangavanhu B 'Impact of the Constitution's normative framework on the interpretation of provisions of the Companies Act 71 of 2008' (2019) 22 *PELJ* 1 15.

https://uwcscholar.uwc.ac.za/home

other words, the constitutional right to privacy would not be available as a remedy against a private party. This would be particularly problematic in the data economy given the rise in power of private actors and the fact that their actions routinely conflict with individuals' rights. On the one hand, the private sector may argue that they have the right to use personal information because this is guaranteed by the freedom of expression or the right to be economically active, and on the other hand, individuals would want to assert their right to privacy. In this regard, Roederer underscores the significance of s 39(2) of the Constitution in resolving private disputes by stating '[i]t is only by looking at the spirit, object and purport of the Bill of Rights that the balancing (mutually limiting) process can make constitutional sense'.[477] Despite the courts having rejected any suggestions of a hierarchy of rights in the Bill of Rights,[478] the right to privacy, more so than the freedom of speech and economic rights, is often linked with preserving dignity in light of South Africa's past social, economic and political inequalities.[479] In contrast, the US tends to promote First Amendment rights, such as freedom of speech, over all other constitutional rights, including dignity.[480]

In a subsequent CC decision, *Khumalo v Holomisa*,[481] the Court held that direct horizontal application of s 8(2) of the Bill of Rights to private disputes may be permitted.[482] To determine whether the fundamental rights ought to apply to private relationships, the CC pointed out that the intensity of the right should be considered, as should the potential invasion of the right by persons other than the state and the nature of the parties.[483] Applying the abovementioned criteria to the right to privacy, it is noted that this right is of particular importance in South Africa's constitutional democracy.[484] First, the right to privacy is recognised as being essential for the preservation of an individual's human dignity, including physical, psychological and

[477] Roederer C 'Post-Matrix Legal Reasoning: Horizontality and the Rule of Values in South African Law' (2003) 19 *South African Journal on Human Rights* 57 76–7.

[478] *NM and Others v Smith and Others (Freedom of Expression Institute as Amicus Curiae)* 2007 (5) SA 250 (CC) para 49. The CC held that one of the main objectives of the struggle against apartheid was the restoration of human dignity.

[479] See also *Khumalo and Others v Holomisa* 2002 (5) SA 401 (CC) para 27. In *Dawood and Another v Minister of Home Affairs and Others; Shalabi and Another v Minister of Home Affairs and Others; Thomas and Another v Minister of Home Affairs and Others* 2000 (3) SA 936 (CC) para 35, the CC held that the Constitution asserts dignity for purposes of reinstatement and reparation of those affected by past injustices while allowing for advancement and transformation going forward.

[480] See 4.6.3 below.

[481] 2002 (5) SA 401 (CC).

[482] 2002 (5) SA 401 (CC) para 33.

[483] 2002 (5) SA 401 (CC) para 33.

[484] See 3.4 above.

https://uwcscholar.uwc.ac.za/home

spiritual well-being.[485] In *NM v Smith*, O'Regan J, in a dissenting opinion, considered the necessity of a constitutional right to privacy and recognised the importance of protecting a personal space in which people could pursue their own goals and foster relationships to the exclusion of the community.[486] Notwithstanding the importance of privacy, in terms of South African privacy jurisprudence, the strength of the right to privacy becomes more attenuated the closer an individual moves into the public sphere and the more social interaction there is.[487] However, this does not mean that the right to privacy is totally relinquished.

Secondly, the use of big data technologies has facilitated extensive intrusions by the private sector into the privacy of individuals. The use of big data analytics facilitates pervasive and potentially privacy-intrusive profiling of individuals, reveals sensitive personal attributes of individuals, and undermines the dignity and autonomy by compromising the ability to exercise control over the processing of personal information.[488]

Thirdly, as was previously stated, the private actors play a prominent and influential role in society. Bilchitz states, with merit, 'their very power to affect the fundamental rights of individuals also provides the basis for a recognition of their obligations to ensure they protect the rights of those same persons'.[489] Therefore, the potential for invasion of privacy by the private sector employing such technologies provides compelling reasons for the direct application of the constitutional right to privacy in such circumstances. It is argued that the Bill of Rights would have less impact if it only applied to vertical relationships, as this could potentially create more opportunities for the private sector to misuse personal information. Therefore, it is no surprise that companies domiciled in the US wield great power in relation to the processing of personal information.[490]

[485] McQuoid-Mason D *The Law of Privacy in South Africa* (1978) xxxix; Burns Y *Communications Law* 3 ed (2015) 229; Van der Bank C (2012) 78.
[486] *NM and Others v Smith and Others (Freedom of Expression Institute as Amicus Curiae)* 2007 (5) SA 250 (CC) para 130.
[487] Mia N 'The Problems with Prince: A critical analysis of Minister of Justice and Constitutional Development v Prince' (2020) 10 *Constitutional Court Review* 401 417; Bilchitz D (2016) 50.
[488] See 2.3.3 above.
[489] Bilchitz D (2016) 54.
[490] See 4.2 below.

https://uwcscholar.uwc.ac.za/home

3.6.3 Subsidiarity

The Constitution is the supreme law of the country and any conduct or law that is inconsistent with the Constitution is invalid.[491] Cachalia and Klaaren state: 'The doctrine of subsidiarity is the founding principle of constitutional supremacy read with its correlate, the judge-made rule of subsidiarity.'[492] The principle of subsidiarity provides that a litigant must rely on the legislation and not directly on the constitutional right unless the litigant is challenging the constitutionality of the subsidiary legislation or requires the Constitution to assist with interpreting such legislation.[493] In *Minister of Health v New Clicks South Africa (Pty) Ltd*,[494] a matter that dealt with administrative justice rights, Chaskalson CJ held that '[a] litigant cannot avoid the provisions of PAJA by going behind it, and seeking to rely on s33(1) of the Constitution or the common law'.[495] In *My Vote Counts NPC v Speaker of the National Assembly*,[496] the CC held that once parliament enacts legislation to fulfil a constitutional right, the legislation becomes the primary mechanism of enforcement and the constitutional right plays only a supporting role.[497] As such, the constitutional right to privacy is, therefore, only a remedy of last resort when other remedies have failed or are inadequate.[498] However, the Constitution remains supreme, albeit in an indirect manner since interpreting any legislation must be done in a manner that promotes constitutional norms and values.[499]

The discourse on POPIA elucidates that its objective is to give effect to the constitutional right to privacy. However, it has also been argued that while there is significant overlap between the right to privacy and data protection, there is also a significant divergence. In this sense, data protection, in contrast to privacy as it is articulated in South Africa, aims to ensure the free flow of information. This free movement of information is important for economic reasons. The need to ensure the availability of personal information has contributed to it becoming an increasingly important asset. Notably, the major legislative instrument for handling personal

[491] Section 2, Constitution.
[492] Cachalia F & Klaaren J (2021) 18.
[493] De Vos P & Freedman W (eds) *South African Constitutional Law in Context* (2014) 586; *My Vote Counts v Speaker of the National Assembly and Others* 2016 (1) SA 132 (CC) para 46.
[494] *Minister of Health and Another v New Clicks South Africa (Pty) Ltd and Others* 2006 (2) SA 311 (CC).
[495] 2006 (2) SA 311 (CC) para 96. Paragraph 95 of the judgement states that 'PAJA is the national legislation that was passed to give effect to the rights contained in section 33'.
[496] 2016 (1) SA 132 (CC).
[497] 2016 (1) SA 132 (CC) para 53.
[498] POPIA was enacted to give effect, or partial effect, to the constitutional right to privacy.
[499] Section 39(2), Constitution; *My Vote Counts v Speaker of the National Assembly and Others* 2016 (1) SA 132 (CC) para 52.

https://uwcscholar.uwc.ac.za/home

information, POPIA, does not see personal information as an economic asset or a kind of property. It is submitted that POPIA, as the legislative framework to enforce the constitutional right to privacy, may not provide the appropriate mechanisms to deal with personal information in such instances. Therefore, it is necessary to assess whether it would be more suitable to consider s 25 of the Constitution in the given circumstances. This aspect will be explored further in chapter six.

3.7 CONCLUSION

Discussions about privacy are often intertwined with technological developments. In this chapter, it was shown that the ongoing and persistent threats presented by technology require that the law of privacy continuously develop and adapt to adequately respond to such dangers. Privacy is an evolving concept shaped by the political and technological characteristics of society at any given time and is therefore not easily defined. Notwithstanding the fact that privacy cannot be satisfactorily defined and despite several attempts to do so, the right to privacy in South Africa is traditionally described in terms of notions such as secrecy and solitude, having been recognised as evolving from a conception of privacy understood as the right to be left alone.

This notion of privacy recognises the presence of the individual's inner sanctuary, which is anticipated to be free from external interference. As the individual's interactions become more public, the expectation of privacy diminishes without being totally obliterated. This interpretation has received judicial endorsement and forms the basis of South African privacy jurisprudence. However, technological developments have raised doubts as to whether a concept of privacy based on secrecy and solitude can offer sufficient legal safeguards for data processing. Efforts to isolate oneself from the outside world in order to maintain a state of seclusion or secrecy by abstaining from the use of technology are neither practical nor realistic. Therefore, the adoption of data protection legislation was necessary to ensure adequate data protection for individuals by granting them a level of control over the processing of their personal data.

Notably, the implementation of POPIA has a dual purpose, namely to give effect to the constitutional right to privacy while facilitating the free flow of information. It is argued that a tension exists between these two objectives. As such, the right to privacy, as articulated in South Africa, is not compatible with the free flow of information. Therefore, despite significant

UNIVERSITY of the WESTERN CAPE
https://uwcscholar.uwc.ac.za/home

overlaps, data protection is irreducible to privacy. It is submitted that the design of POPIA, in part, stems from economic considerations and that its other stated purpose, the free flow of information, has encouraged the tradeability of personal information and its treatment as an economic asset. As a result, private sector actors' threats to individuals' fundamental rights have brought attention to their control and influence.

This argument presents conceptual difficulties for the current data protection framework, as POPIA was not designed to treat personal information as a form of property. As such, it is submitted that POPIA cannot adequately deal with the commodification of personal information. However, South Africa has adopted a transformative constitution that encompasses several features, such as horizontality and subsidiarity, which allow for constitutional norms to apply to both public and private bodies. Transformative constitutionalism dictates that the Constitution remain relevant and adapt to emerging challenges to meet the needs of society.

The shortcomings of existing data protection rules have raised questions about whether an alternative regulatory system based on property rights in personal data could be more suitable. The next chapter examines the privacy discourse and the debate on property rights in personal information from a US perspective.

UNIVERSITY of the
WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

CHAPTER FOUR: THE PROPERTISATION OF PERSONAL INFORMATION FROM A UNITED STATES PERSPECTIVE

4.1 INTRODUCTION 97

4.2. MARKETPLACE DISCOURSE 98

4.3 RIGHT TO BE LET ALONE AND THE SECRECY PARADIGM 102

4.4 REGULATION OF DATA PROTECTION IN THE US 103

4.5 LAW OF TORT 105

4.5.1 Intrusion tort 106

4.5.2 Public disclosure of private facts 108

4.5.3 Appropriation of name or likeness 110

4.6 AMERICAN CONSTITUTIONAL LAW 113

4.6.1 Substantive due process clause of the Fourteenth Amendment 114

4.6.2 The Fourth Amendment 117

4.6.3 The First Amendment 119

4.7 STATUTORY DATA PROTECTION LAWS 121

4.7.1 Code of Fair Information Practices 122

4.7.2 Federal Trade Commission 124

4.7.3 Selected federal statutes 127

4.7.4 California Consumer Privacy Act (CCPA) 128

4.8 REMARKS 130

4.9 PROPERTY RULES FOR PERSONAL INFORMATION 131

4.9.1 Economic arguments for Propertisation 132

4.9.2 Overview of property rules 132

4.9.3 Significance of ownership 134

4.10 CHARACTERISTICS OF PROPERTISED PERSONAL INFORMATION 135

UNIVERSITY of the WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

4.10.1 Alienability 135
4.10.2 Excludability 138
4.11 CONCLUSION 140

UNIVERSITY of the
WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

4.1 INTRODUCTION

The growth of the US personal data marketplace is driven by big data technologies, a vital cog in US economic growth and development. An enabling regulatory environment has made it possible for US-based technology and data companies to flourish, contributing significantly to the economy. Promoting the free flow of data, a core feature underpinning a free market, creates opportunities for innovative business models built on the collection and analysis of personal data. Conceptually, personal data is viewed in the US as a commodity.[500] This is reflected in the US approach to data protection, which results in the individual being protected as a consumer in the personal data marketplace.[501]

This suggests that the individual is viewed as someone who can exchange his personal information for products or services. Unsurprisingly, the California Consumer Privacy Act (CCPA),[502] which is touted as the US equivalent of the GDPR,[503] refers to the rights of the 'consumer'. Moreover, the CCPA defines the terms 'sell', 'selling', 'sale', or 'sold' to mean selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating verbally, in writing, or by electronic or other means, a consumer's personal information by a business to another business or a third party for monetary or other valuable gain.[504] This, unequivocally, suggests that personal information is a commodity. Due to the specificities of the US legal system and the divergent approaches to data protection, it is not possible for South Africa to simply adopt a US approach. However, the personal data trade is a universal phenomenon, and the US discussion on the propertisation of personal information may provide valuable guidance for the South African context.

The ensuing discussion in this chapter commences with a discussion on the treatment of personal data in a market-driven discourse, as in the US. Then, an overview of the legislative framework for dealing with data protection in the US is discussed. First, the analysis focuses on the origins of US privacy law and how the initial philosophies and beliefs were adapted to deal with the concerns related to data processing brought about by technological advancements. Secondly, US data protection, or 'information privacy' as it is more commonly known, is

[500] Schwartz P & Peifer K 'Transatlantic data privacy law' (2017) 106 *Georgetown Law Journal* 115 121.
[501] Schwartz P & Peifer K (2017) 121; Baik J 'Data Privacy against Innovation or against Discrimination?: The Case of the California Consumer Privacy Act (CCPA)' (2020) 52 *Telematics and Informatics* 1 2.
[502] CCPA of 2018. See 4.7.4 for a discussion on the CCPA.
[503] Baik J 'Data Privacy against Innovation or against Discrimination?: The Case of the California Consumer Privacy Act (CCPA)' (2020) 52 *Telematics and Informatics* 1 2.
[504] Section 1798.140(t)(1), CCPA.

https://uwcscholar.uwc.ac.za/home

discussed, specifically its roots in tort law and in the US Constitution. It is argued that the law of tort and the constitutional law of privacy have proved ineffective in providing safeguards to protect privacy from the advancements in computer technology and, more recently, big data technologies. Consequently, various sector-specific laws have been enacted to deal with the dangers increasingly posed by advancing technologies, which has resulted in a muddled, inconsistent patchwork of torts, constitutional, and statutory laws, leaving significant gaps in data protection. To overcome the shortcomings of the US data protection regime, the propertisation of personal information was suggested as an alternative to acknowledge the commodification thereof and better handle the challenges posed by the information revolution. It is argued that the institution of property is expected to provide a framework to efficiently regulate the use of resources, namely, personal information.

4.2. MARKETPLACE DISCOURSE

Technology is a key economic driver and contributor to the strength of the US economy, and the impact of big data, IoT, cloud computing, and similar technologies affect numerous sectors and industries.[505] The US government wants to establish a regulatory framework that encourages the growth of technology and data companies. [506] It was estimated that the value of the US data economy in 2022 was approximately €242 358 billion.[507] The data harvesting industry is experiencing rapid growth in the US.[508] According to Burns and Burger-Smidt, the processing and analysis of big data in the US dwarfs the scale of processing occurring in South Africa.[509] However, it is argued that the volume of processing that occurs is inconsequential, as it does not diminish the impact of the problem or reduce its significance.

The increase in data collection and analysis of personal information fosters economic activity and offers potential benefits and advantages for consumers, companies and government alike.[510] A preference for the free flow of information over personal privacy is a central feature

[505] Deutsch A 'The 5 Industries driving the US economy' *Investopedia* 17 September 2020 available at https://www.investopedia.com/articles/investing/042915/5–industries–driving–us–economy.asp (accessed 26 September 2020).
[506] Schwartz P & Peifer K (2017) 137.
[507] EC *European Data Market Study 2021–2023* (2023) 147.
[508] Shapiro R & Aneja S *Who Owns Americans' Personal Information and What Is It Worth?* (2019) 4.
[509] Burns Y & Burger-Smidt A *Protection of Personal Information: Law and Practice* 2 ed (2023) 789.
[510] White House *Big Data: Seizing Opportunities, Preserving Values* (2014) 5–6; King N & Forder J 'Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data' 32 *Computer Law & Security Review* 696 696.

https://uwcscholar.uwc.ac.za/home

of US marketplace discourse.[511] The free flow of information is guaranteed by the First Amendment to the US Constitution.[512] In contrast to South Africa and the EU, the US Constitution does not expressly provide for a constitutional right to privacy.[513] This disparity may provide a clue as to why, in the US, there is a preference for the preservation of freedom of speech over the safeguarding of privacy.

Traditionally, the US has been reluctant to implement omnibus privacy legislation at the federal level to regulate the commercial collection and use of personal information.[514] The US Senate proposed an omnibus legislative bill in the mid-1970s to regulate automated and manual processing of personal data by all levels of government and the private sector.[515] Ultimately, a weakened form of legislation was passed in the form of the Privacy Act of 1974, which applies only to the processing of personal data by federal agencies.[516] The promise of economic benefits and the positive impact of technology companies on the economy have been cited as reasons for the apparent lack of political will to regulate the processing of personal data by the private sector.[517] Consequently, the processing of personal data by the private sector is largely self-regulated as will be discussed below.[518]

UNIVERSITY of the
WESTERN CAPE

The availability of personal information, combined with the increasingly sophisticated analytical techniques made possible by technology, drives innovative progress.[519] Personal information supports an advertising marketplace that makes it possible for the consumer to benefit from free online services and content.[520] As a result, the US adopts a policy of promoting and strengthening trust among consumers to encourage the uptake of innovative technologies from which consumers can derive benefit. By encouraging trust rather than

---

[511] Schwartz P & Peifer K (2017) 137.

[512] The US Constitution Amendment I read: 'Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.'

[513] See 4.6 below.

[514] Aretz Y & Strandburg K (2020) 258. Martin N et al 'How data protection regulation affects startup innovation' (2019) 21 *Information Systems Frontiers* 1307 1308 explain that regulations refer to any general form of 'coercive rule setting' by governments to influence market activity and economic actors.

[515] Lynskey O *The Foundations of EU Data Protection Law* (2015) 17.

[516] Solove D 'A brief history of information privacy law' (2016) *Proskauer on Privacy, PLI* 1 26.

[517] Litman J 'Information privacy/information property' (2000) 52 *Stanford Law Review* 1283 1291; Schwartz P & Peifer K (2017) 137.

[518] See 4.7 below.

[519] White House 'Consumer data privacy in a networked world: A Framework for protecting privacy and promoting innovation in the global digital economy White House report' (2012) 4 *Journal of Privacy and Confidentiality* 95 99.

[520] White House (2012) 99.

https://uwcscholar.uwc.ac.za/home

implementing privacy regulations, it is clear the aim is to maximise economic gains at an acceptable level of risk to individual privacy.

Goldfarb and Tucker recognise that the data economy offers several advantages for individuals and businesses.[521] Businesses may gain access to large volumes of potentially monetizable personal data, while individuals may benefit from free products. Therefore, they also see an inherent tension between innovation and consumer privacy.[522] Zarsky explains that this tension stems from the benefits that may be derived from the development of innovative technologies and business models and the extent to which privacy laws could affect the flow of information necessary for such innovation.[523] Increased regulation may stifle innovation by limiting potentially innovative paths and/or increasing innovation costs.[524] The rhetoric, according to Aretz and Strandburg, in dismissing calls for heightened privacy regulations, goes as follows:[525]

> 'The information economy is the lifeblood of US economic growth. Increasingly, it runs on personal information collected and aggregated by companies as they provide us with services. The use of this information has brought us many benefits and conveniences and is the mainstay of our most successful companies. Sure, each of us might, in principle, prefer not to have our own activities tracked, but do we really want to risk stalling out the engine of our innovative economy by imposing privacy regulations?'

As value creation may be contingent on secondary applications of personal information,[526] regulations that are too restrictive could throttle innovation, negatively impacting revenue growth and depriving consumers of innovative goods and services. The US government promotes the importance of trust in maintaining social and economic benefits and aims to safeguard consumer trust and foster innovation by implementing consistent privacy regulations and reducing compliance burdens for both consumers and companies.[527] Therefore, innovation considerations feature prominently in the US when contemplating privacy regulations.[528]

---

[521] Goldfarb A & Tucker C 'Privacy and innovation' (2012) 12 *Innovation Policy and the Economy* 65 66–7.
[522] Goldfarb A & Tucker C (2012) 65 66–7.
[523] Zarsky T 'The Privacy-Innovation Conundrum' (2015) 19 *Lewis & Clark Law Review* 115 118, 140.
[524] Aretz Y & Strandburg K (2020) 2.
[525] Aretz Y & Strandburg K (2020) 259.
[526] See 2.3.4.5 above.
[527] White House (2012) 95–103; White House (2014) 11.
[528] Zarsky T (2015) 119.

https://uwcscholar.uwc.ac.za/home

Implicit in the US approach is the trade-off between innovation and privacy. According to Cofone, this trade-off is often depicted as a choice between rights and efficiency.[529] Cohen explains that the purpose of US privacy laws is to not only protect individuals but to further public policy goals relating to, among other things, innovation and human flourishing.[530] This underlying philosophy dictates that increased privacy protections should not impede innovation and the ability to design new offerings for consumers, and that any privacy framework so implemented must be flexible enough to permit and encourage innovation.[531] Such an approach is embraced by the Obama Administration which states that: 'No matter how serious and consequential the questions posed by big data, this Administration remains committed to supporting the digital economy and the free flow of data that drives its innovation.'[532]

The rights-bearer of US privacy protection is therefore a consumer who benefits from the presence of innovative technologies and merits protection from market failures.[533] In this regard, personal information supports an advertising marketplace that makes it possible for the consumer to benefit from free online services and content.[534] Privacy, from a US perspective, is not so much about safeguarding the individual's rights as it is about ensuring the individual's autonomy to enter into transactions relating to his personal data. In other words, privacy, in essence, seeks to establish a setting where individuals can exercise their autonomy free from external interference. Therefore, it is questionable whether an adequate balance can be achieved between innovation and consumer privacy. Moreover, it underscores the importance of personal information as a valuable economic resource from which to generate value.

It is submitted that the emphasis placed on the free flow of data to drive economic growth as opposed to prioritising privacy rights has had a noticeable impact on shaping the US approach to data protection, as is reflected in the patchwork legislation that will be discussed later in this chapter.[535] In contrast, the recognition of dignity, privacy and data protection as fundamental rights, such as in South Africa and the EU, has led to the promulgation of omnibus legislation that regulates personal information as a broad category rather than regulating personal

[529] Cofone I 'The dynamic effect of information privacy law' (2017) 18 *Minnesota Journal of Law, Science & Technology* 517 521.
[530] Cohen J 'What privacy is for' (2013) 126 *Harvard Law Review* 1904 1927.
[531] FTC *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers* (2012) 7–9.
[532] White House (2014) 9.
[533] Schwartz P & Peifer K (2017) 137.
[534] White House (2012) 99.
[535] See 4.7 below.

https://uwcscholar.uwc.ac.za/home

information based on sectoral or industry considerations.[536] The objectives of the contrasting approaches will have a direct bearing on the adequacy of the privacy safeguards implemented.[537] Marketplace discourse lends itself to the idea that personal information is a commodity in the market and that human flourishing is furthered to the extent that individuals can maximise their preferences regarding data exchanges free from legal constraints.[538] In this regard, it is submitted that the ideals of liberty and freedom have a greater significance in the US compared to the importance given to dignity in South Africa and the EU.[539]

In the US, there has been an absence of a coherent understanding of the nature of information privacy interests and the legal theory that should find application in that context.[540] The following section delves into the theoretical rationales that underpin the US data protection legal framework.

4.3 RIGHT TO BE LET ALONE AND THE SECRECY PARADIGM

The foundation of US privacy laws, like South Africa, is premised on the right to be left alone and the recognition of an individual's 'inviolate personality'.[541] As such, the historical roots of the right to privacy from a US perspective are based on the idea that private information ought to be free from public scrutiny. Like South Africa, the concept of the 'right to be left alone' is based on the idea of a 'secrecy paradigm'.[542] This implies a privacy entitlement in the non-divulgence of personal information. As a result, any partial or complete disclosure of information by a person represents a renunciation of privacy rights, and there is no reasonable expectation of privacy in information that is not kept secret.[543]

[536] See 3.3.3 and 5.3.3 for an overview of POPIA and the GDPR respectively.

[537] This will also determine how the courts in the various jurisdictions approach cases that require a balancing between privacy and free speech.

[538] Schwartz P & Peifer K (2017) 132.

[539] See 3.3.2 above for the South African perspective. See also 5.1 below for the EU perspective.

[540] Bergelson V 'It's personal but is it mine? Toward property rights in personal information' (2003) 37 *University of California Davis Law Review* 379 400.

[541] See 3.2.1 above.

[542] Bergelson V (2003) 401.

[543] Jerome J 'Big Data: Catalyst for a Privacy Conversation' (2014) 48 *Indiana Law Review* 213 225; Solove D *The Digital Person: Technology and Privacy in the Information Age* (2004) 198–99; *Katz v United States* (1967) 389 US 347 351.

https://uwcscholar.uwc.ac.za/home

The privacy-as-secrecy conception, described as 'a discrete commodity, possessed absolutely or not at all',[544] suffers serious shortcomings that renders it unhelpful in a modern, technological era. For instance, this conception does not provide for adequate data protection to deal with modern information practices and be responsive to the new challenges created by the Internet.[545] As previously mentioned, the use of smart devices, the miniaturization of sensors in everyday objects, and their proximity to people's bodies enable continuous monitoring of peoples' activities and behaviours, leading to the generation of personal data.[546] These technologies are an integral part of modern-day living, and 'we conceive of them often as a central part of our "private world" through which we conduct our "private" business'.[547] It is submitted that individuals expect privacy despite the widespread disclosure and/or exchange of personal information.[548] Moreover, big data analytics use seemingly innocuous pieces of information to generate comprehensive records about individuals, which may not be perceived as falling within the intimate privacy sphere of the individual.[549] Since data collection is so engrained in modern-day data practices, this raises doubts as to whether a US conception of privacy based on concealing information in today's data-driven economy remains relevant. In this regard, it is reasonable to assume that the conclusion reached in the South African context would be equally applicable to the US insofar as it relates to understanding the implications of privacy conceived as the right to be left alone.[550]

UNIVERSITY of the
WESTERN CAPE

4.4 REGULATION OF DATA PROTECTION IN THE US

Conceptualising privacy as secrecy has significantly influenced the development of US information privacy laws, the effects of which have resulted in considerable limitations with respect to the capacity of the country's legal rules to deal with the challenges of modern data flows. Purtova postulates that the origin of the idea of propertisation of personal information in the US is largely a result of the inability of US data protection laws to adequately respond

[544] Purtova N 'Property rights in personal data: Learning from the American discourse' (2009) 25 *Computer Law and Security Review* 507 513.
[545] See also 3.3.1 above.
[546] See 2.2.4 above.
[547] Bilchitz D 'Privacy, surveillance and the duties of corporations' (2016) 1 *TSAR* 45 45.
[548] See 3.3.1 above.
[549] See 2.3.3 above. See also Schwartz P 'Internet privacy and the state' (1999) 32 *Connecticut Law Review* 815 818.
[550] See 3.3.2 above.

https://uwcscholar.uwc.ac.za/home

to the challenges of technological innovation and the concomitant information flows.[551] This is because the 'dominant language' of US privacy regulations labels the individual as a 'customer' in the marketplace.[552] The individual is deemed to be in a position to exchange or trade anything provided it is not prohibited by law. The effect is that anything that is capable of being exchanged, including personal information in this instance, can become commoditised, necessitating the need for an alternative means of regulation should the prevailing rules prove inadequate.

According to Bergelson, US data protection law resembles 'a patchwork of uneven, inconsistent, and often irrational federal and state rules'.[553] Similarly, Purtova states that US information privacy law does not have a single hierarchical order of rules but comprises a patchwork of rules consisting of tort, constitutional and statutory laws.[554] Solove characterises data protection in the US as using whatever is at hand to address the problems posed by the information revolution.[555] Roos notes that these various laws have proved to be ineffective in dealing with the threats posed to data privacy by technology.[556] The sections that follow will discuss the shortcomings of each of the various types of laws.

It was envisaged that the perceived handicap of the US legal and political system would be remedied by the granting of property rights in personal information.[557] The aim of instituting property rights in personal information is to give people some control over it and improve the overall data protection system.[558] The notion of control conforms to the Westin definition of privacy.[559] According to Westin's definition, ultimate control over personal data rests with the individual to whom it belongs. Therefore, the decision about what information, how much information, and to whom to communicate it rests with the individual. It is submitted that, in the South African context, Westin's understanding of privacy appears to align with that of Neething and Roos.[560] In terms of property, we might interpret the concept of control as being

[551] Purtova N (2009) 508.
[552] Schwartz P & Peifer K (2017) 132.
[553] Bergelson V (2003) 391.
[554] Purtova N (2009) 509.
[555] Solove D 'Privacy and power: Computer databases and metaphors for information privacy' (2001) 53 *Stanford Law Review* 1393 1393.
[556] Roos A *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* (unpublished LLD thesis, University of South Africa, 2003) 27.
[557] Purtova N (2009) 508.
[558] Solove D (2001) 1446; Purtova N (2009) 507.
[559] Westin A *Privacy and Freedom* (1967) 7.
[560] See 3.2.1 and 3.2.2 above.

https://uwcscholar.uwc.ac.za/home

synonymous with ownership, suggesting the right to trade and exchange personal information in the 'privacy market'.[561] Following such reasoning, default ownership would vest in the individual. In this regard, Laudon envisions a personal information market that is based on individual ownership of personal information and in which individuals can receive fair compensation for the use of their personal information by others.[562]

The following sections discuss the 'patchwork' of laws that comprise the US data protection regime. The analysis focuses on the law of torts,[563] the US Constitution,[564] and a selection of sectoral laws.[565] The purpose of the discussion is to provide a basis for the subsequent discussion on the propertisation of personal information. The privacy-as-secrecy conception has influenced the development of data protection principles, and consequently, it has become challenging for the available legal mechanisms to deal with modern information practices that extend beyond issues of privacy. The discussion will entail looking at how the various laws function and their shortcomings in responding to modern day challenges.

UNIVERSITY of the
WESTERN CAPE

4.5 LAW OF TORT

Since the turn of the twentieth century, US courts and legislatures have adopted the Warren and Brandeis 'right to privacy' conception.[566] In doing so, they granted protection to persons against a variety of privacy invasions.[567] Various scholars have examined the role of tort in resolving the data protection problem and information misuse and have concluded that the existing scheme of privacy torts is limited and inadequate.[568] To this end, Ludington, for example, comments:[569]

---

[561] Lazaro C & Le Métayer D 'The control over personal data: True remedy or fairy tale?' (2015) 12 *SCRIPTed* 3 8–9. See also Solove D (2001) 1446.

[562] Laudon K 'Markets and privacy' (1996) 39 *Communications of the ACM* 92 93. Examples of personal data marketplaces currently facilitating the trading of personal data are metaMe.com, Humanity.com and Datum.org.

[563] See 4.5 below.

[564] See 4.6 below.

[565] See 4.7 below.

[566] See 4.3 above.

[567] Solove D (2001) 1432; Nehf J 'Recognizing the societal value in information privacy' (2003) 78 *Washington Law Review* 1 29–30.

[568] Murphy R 'Property rights in personal information: An economic defense of privacy' (1996) 84 *Georgetown Law Journal* 2381 2388–93; Ludington S 'Reining in the data traders: A tort for the misuse of personal information' (2006) 66 *Maryland Law Review* 140 145; Purtova N (2009) 509; Rabin R 'Perspectives on privacy, data security, and tort law' (2017) 66 *DePaul Law Review* 313 324–25.

[569] Ludington S (2006) 159.

https://uwcscholar.uwc.ac.za/home

> 'To suggest that the existing scheme of privacy torts would be an effective tool for addressing the complex problems of personal information is akin to suggesting that one could use a toy drill to fix a nuclear reactor.'

The law of tort has been developed by courts through a system of precedent, but due to the constitutional division between federal and state powers in the US, it is mainly state law, resulting in a lack of uniformity and agreement on fundamental principles regarding common law between states.[570] In 1960, Prosser concluded that the overwhelming majority of US courts recognised the right to privacy in one form or another.[571] Prosser isolated four distinct torts for invasion of privacy interests, namely,

- intrusion upon the plaintiff's seclusion or solitude, or into his private affairs;
- public disclosure of embarrassing private facts about the plaintiff;
- publicity that places the plaintiff in a false light in the public eye; and
- appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

Prosser's framework was adopted by the American Law Institute,[572] which produced the Restatement of the Law of Torts (Restatement), a non-binding but highly persuasive attempt to clearly and concisely set out the principles of tort to overcome the variations and the lack of uniformity between US states.[573] In the following subsections, only those torts that are most relevant to the processing of personal information will be discussed.

4.5.1 Intrusion tort

The tort of intrusion upon seclusion protects against intentional interference, whether physical or otherwise, in a manner that is 'highly offensive to a reasonable person,' upon another's interest in 'solitude or seclusion' or 'private affairs or concerns.'[574] The intrusion tort provides

[570] Purtova N (2009) 509.

[571] Prosser W 'Privacy' (1960) 48 *California Law Review* 383 386.

[572] The official website of the American Law Institute is available at *https://www.ali.org/* (accessed 29 October 2020).

[573] Purtova N (2009) 509. See also Eades R 'Attempts to federalize and codify tort law' (2000) 36 *American Bar Association* 1 8–9. There are, however, instances where different states have adopted the law of torts or elements thereof. For example, in *Howard v Aspen Way Enterprises, Inc* (2017) 406 P3d Wyo 1271, the Supreme Court of Wyoming adopted the elements of the invasion-of-privacy tort of intrusion upon seclusion as set forth in s 652B Restatement (Second) of Torts and in *McElhaney v Thomas* (2017) 405 P3d Kan 1214, the Supreme Court of Kansas adopted the standards set forth in the Restatement (Second) of Torts. This would ensure some uniformity and certainty in applying the law.

[574] Section 652B, Restatement (Second) of Torts.

https://uwcscholar.uwc.ac.za/home

a potential remedy for the recovery of an unauthorised acquisition or transfer of personal information.[575] Intrusion is not limited to that of a physically defined space and can encompass intangible interests such as personal information.

Purtova submits, correctly, in my view, that it is difficult to apply the intrusion tort to new information practices.[576] Due to the intrusion tort's concept of invasion of seclusion, information collection and use taking place over the Internet could be considered public conduct.[577] It is submitted that processing information divulged voluntarily by an individual or compiling information from publicly available records does not constitute an intrusion, as the intrusion tort generally only protects information that has been kept secret.[578] This view is supported by the decision in *Dwyer v American Express Co.* (*Dwyer*).[579] In *Dwyer*, a group of American Express clients instituted legal proceedings against the company to challenge the company's profiling practices and its disclosure of cardholder information, such as spending habits, to third parties. The clients claimed that the disclosure of the information by the company constituted an intrusion upon their seclusion.[580] The court held that the information practices did not constitute an intrusion upon seclusion, as the clients could not establish that the disclosure by the company was unauthorised.[581] The court reasoned that by using the card, the clients voluntarily gave the company the information that revealed their spending habits.[582] In doing so, the company merely compiled voluntarily given information, which it then rented out to third parties.[583] The decision in *Dwyer* therefore suggests that an individual cannot have an expectation of privacy in personal information that has been willingly and voluntarily disclosed.[584] It also means that once consent is given, the company may use the information as

[575] Murphy R (1996) 2391; Bergelson V (2003) 405; Zhu B 'A traditional tort for a modern threat: Applying intrusion upon seclusion to dataveillance observations' (2014) 89 *New York Law Review* 2381 2384.
[576] Purtova N (2009) 509.
[577] Solove D (2001) 1432–33.
[578] Zhu B (2014) 2385.
[579] (1995) 652 N.E. 2d Ill App Ct 1351.
[580] (1995) 652 N.E. 2d Ill App Ct 1351 1352–54.
[581] (1995) 652 N.E. 2d Ill App Ct 1351 1354.
[582] (1995) 652 N.E. 2d Ill App Ct 1351 1354. The court held:
> 'By using the American Express card, a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences. We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation.'

[583] (1995) 652 N.E. 2d Ill App Ct 1351 1354.
[584] Ludington S (2006) 161.

https://uwcscholar.uwc.ac.za/home

it wishes. The intrusion tort therefore does not provide the data subject with the means to limit the processing of personal information.[585]

In the context of data protection, the use of the intrusion tort is limited by the requirement that the privacy intrusion must be 'highly offensive to a reasonable person', as in most instances the information being collected is often innocuous and seemingly harmless.[586] To determine whether an intrusion is sufficiently offensive, one must consider 'the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded'.[587] Solove comments that the threshold for meeting such requirements would be difficult as the problem emerges through the aggregation of information over a period of time.[588]

4.5.2 Public disclosure of private facts

The disclosure tort provides a remedy against the public disclosure of a private matter that is 'not of legitimate concern to the public' and the publication of which 'would be highly offensive to a reasonable person'.[589] The disclosure tort requires the widespread publication of personal information. Information must be communicated to a sufficient number of people so that it is 'substantially certain to become one of public knowledge'.[590] However, knowledge regarding the sale, transfer, and disclosure of personal information between parties is ordinarily restricted to those parties.[591] Bergelson states that it is a matter of degree as to how many persons the information was made known to in order to constitute the 'public'.[592]

The public disclosure tort protects only 'highly offensive' personal information. The publication of information typically found in a database, such as names, birthdates, addresses, and telephone numbers, is not considered to be highly offensive if made public.[593] Disclosure of personal information becomes highly offensive if it concerns private facts that are not in the

[585] See also the discussion in 3.3.1 on the common law protection of privacy in the South African context.
[586] Solove D (2004) 59; Zhu B (2014) 2385.
[587] *Remsburg v Docusearch, Inc* (2003) 816 A.2d NH 1001 1008–9.
[588] Solove D (2001) 1432.
[589] Section 652D, Restatement (Second) of Torts.
[590] Section 652D comment a, Restatement (Second) of Torts.
[591] Purtova N (2009) 510.
[592] Bergelson V (2003) 408.
[593] Ludington S (2006) 164; Solove D (2004) 60.

https://uwcscholar.uwc.ac.za/home

public domain and is retained by the plaintiff 'entirely to himself or at most revealed only to his family or to close friends'.[594] Purtova concludes, with merit, that even if a plaintiff can establish that the publication of personal information is highly personal or embarrassing, the plaintiff cannot rely on the public disclosure tort if he publishes this information on the Internet.[595] Similarly, the publication of facts in public records is not private facts and is therefore not actionable.[596]

In a comment to the public disclosure tort, the Restatement states:[597]

> 'The protection afforded to the plaintiff's interest in his privacy must be relative to the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbors and fellow citizen. Complete privacy does not exist in this world except in a desert, and anyone who is not a hermit must expect and endure the ordinary incidents of the community life of which he is a part.'

Technological and marketing developments have altered boundaries concerning habits, attitudes, and what is acceptable in data processing. Ludington refers to today's society as a 'full-disclosure society', where it has become acceptable for people to reveal their most embarrassing secrets.[598] Technological developments constantly challenge privacy expectations and norms, changing social behaviours and privacy infringements, as well as people's tolerance levels for such infringements.[599] Individuals sharing personal information on social media is now commonplace in comparison to the pre-social media age, when it was unusual for people to do so in a public arena. People today still expect privacy in terms of who will use their information and for what purposes after sharing it.

As was mentioned in chapter two,[600] individuals generally lack knowledge about who possesses their personal data and how it is being used.[601] Murphy states, with merit, that although the disclosure tort aims to protect information privacy, such protection is

---

[594] Section 652D comment b, Restatement (Second) of Torts.
[595] Purtova N (2009) 511. See also Ludington S (2006) 165.
[596] Section 652D comment b, Restatement (Second) of Torts. See also McNulty P 'The public disclosure of private facts: There is life after Florida Star' (2001) 50 *Drake Law Review* 93 102.
[597] Section 652D comment c, Restatement (Second) of Torts.
[598] Ludington S (2006) 165.
[599] Abril P 'Recasting Privacy Torts in a Spaceless World' (2007) 21 *Harvard Journal of Law and Technology* 1 11; Papadopoulos S 'Revisiting the Public Disclosure of Private Facts in Cyberworld' (2009) *Obiter* 30 40.
[600] See 2.3.2 and 2.3.3 above.
[601] Mundie C 'Privacy pragmatism: Focus on data use, not data collection' (2014) 93 *Foreign Affairs* 28 31–2.

https://uwcscholar.uwc.ac.za/home

ineffective.[602] Two reasons can be identified. First, the sale or transfer of personal information between companies and third parties is often done in secret without individuals being aware of the transactions linked to their personal data.[603] Bergelson concludes that the transfer of personal information from a primary collector to the secondary market is unlikely to be considered public disclosure.[604] Therefore, the requirement that the private matter be made public will not be met. Secondly, information is readily available in the public domain for companies to use for profiling purposes. This information is often factual and innocuous. It is submitted that the disclosure tort fails to offer protection when the individual is unaware of the processing and when it involves the processing of publicly available information.

4.5.3 Appropriation of name or likeness

The appropriation tort protects individuals against the appropriation or exploitation of their name or likeness by another for his own use or benefit.[605] Appropriation is often conflated with the right to publicity, the former providing a remedy to protect the interests that a non-famous individual has in the exclusive use of his own identity, while the latter grants a property right to celebrities for them to exploit the value of their identity.[606] Some scholars state that the terms 'appropriation' and 'right to publicity' are used interchangeably throughout the US.[607] The appropriation tort could conceivably apply to data processing since appropriation implies some sort of use that is akin to processing, while the name or likeness of a person could constitute personal data.[608] Solove suggests that the appropriation tort may be applied to the use of targeted marketing, which can be seen as using another person's personal data for profit or commercial gain.[609]

There have been various unsuccessful attempts to extend the application of the appropriation tort to the unauthorised dissemination and uses of personal data.[610] In *Shibley v Time, Inc.*,[611]

[602] Murphy R (1996) 2392.
[603] Solove D 'Privacy and power: Computer databases and metaphors for information privacy' (2001) 1433.
[604] Bergelson V (2003) 410.
[605] Section 652C, Restatement (Second) of Torts.
[606] Section 652C comment c, 'Restatement (Second) of Torts; Ludington S (2006) 166–67.
[607] Bergelson V (2003) 410–11; Ludington S (2006) 167; Purtova N (2009) 511.
[608] Lim H 'The data protection paradigm for the tort of privacy in the age of big data' (2015) 27 *Singapore Academy of Law Journal* 789 814.
[609] Solove D (2001) 1434.
[610] Bergelson V (2006) 411; Purtova N (2009) 511.
[611] (1975) 341 NE 2d Ohio Ct App 337.

https://uwcscholar.uwc.ac.za/home

a class action based on appropriation was instituted against several magazines and the issuer of American Express credit cards who sold subscription lists to direct mail companies without the prior consent of the subscribers.[612] The Court dismissed the appropriation claim on the basis that the subscribers did not have a protected privacy interest in their personal information and held that appropriation may only be invoked 'where the plaintiff's name or likeness is displayed to the public to indicate that the plaintiff endorses the defendant's product or business'.[613] Similarly in *Dwyer*, the court held that 'an individual name has value only when it is associated with one of defendants' lists' and that 'defendants create value by categorizing and aggregating these names'.[614]

In *Fraley v Facebook, Inc.* (*Fraley*),[615] the plaintiffs instituted a class action against Facebook, alleging that the names and likenesses of the plaintiffs were misappropriated to promote products and services through an advertising service called the 'Sponsored Stories' programme.[616] Facebook generates revenue by selling targeted advertising.[617] Although the parties settled the matter, the court noted that the plaintiffs had asserted sufficient economic injury for a claim to proceed by making specific allegations of harm that were not just hypothetical or potential but 'concrete and particularized'.[618]

UNIVERSITY of the
WESTERN CAPE

In *Rojas-Lozano v Google, Inc. (Rojas-Lozano)*,[619] the plaintiff instituted action against Google based on unfair practises and unjust enrichment, alleging that Google profited off the 'free labor' of users through its 'reCAPTCHA' programme during Gmail sign-ups.[620] The Automated Public Turing test to tell Computers and Humans Apart or 'CAPTCHA' for short, is a website security measure aimed at distinguishing humans visiting a website from automated programmes and requires them to decipher words or numbers displayed as distorted images.[621] Google's reCAPTCHA service prompts a user to type two words that are displayed in two distorted images, the contents of which cannot be recognised by automated programs.[622]

---

612 (1975) 341 NE 2d Ohio Ct App 337 340.
613 (1975) 341 NE 2d Ohio Ct App 337 339.
614 *Dwyer v American Express Co* (1995) 652 NE 2d Ill App Ct 1351 1356. See also 4.5.1 above.
615 (2011) 830 F Supp 2d NC Cal 785.
616 (2011) 830 F Supp 2d NC Cal 785 791.
617 (2011) 830 F Supp 2d NC Cal 785 790.
618 (2011) 830 F Supp 2d NC Cal 785 797.
619 (2016) 159 F Supp 3d ND Cal 1101.
620 (2016) 159 F Supp 3d ND Cal 1101 1107–08.
621 (2016) 159 F Supp 3d ND Cal 1101 1107.
622 (2016) 159 F Supp 3d ND Cal 1101 1107.

https://uwcscholar.uwc.ac.za/home

The first word identifies that the Web user is not a robot, and the other is a word that Google's character recognition technology uses to improve Google Books and Google Maps.[623] In so doing, Google uses the actions of the user to read and transcribe images for its own commercial use and benefit. In contrast to *Fraley*, the Court in *Rojas-Lozano* dismissed the action brought by the plaintiff as she failed to demonstrate that typing the second word for the purposes of opening a free Gmail account was something for which a reasonable consumer would expect to receive compensation.[624]

Rabin states, with merit, that while the appropriation tort may offer a plaintiff privacy protection against commercial appropriation, the plaintiff must demonstrate that the use of their personal data generated an economic benefit to which they would be entitled.[625] This is particularly problematic given that the commodification of personal data is widespread. Since the appropriation tort places the onus on the plaintiff to prove that their personal data has economic value, it is reasonable to argue that the tort fails to recognise the realities of current data practices and is therefore ill-suited to provide the necessary relief in response to the modern challenges brought about by technological advancements. In contrast, data protection legislation, such as POPIA and GDPR, shifts the responsibility of demonstrating that processing is lawful to the data processors.[626]

UNIVERSITY of the
WESTERN CAPE

The appropriation tort applies to individuals that have prestige or value associated with their name or identity but are generally not ordinary individuals.[627] Although it is correct to assume that most individuals attach some value to their personal data, this value is more likely rooted in dignity and privacy interests than commercial considerations. In comparison to other torts, the appropriation tort can protect pecuniary interests in the commercial exploitation of identity and can therefore be understood in property terms. This is particularly significant for the purposes of this dissertation because personal data, as an aspect of privacy and thus personality, is generally considered non-patrimonial in nature. Since identity, as an aspect of personality rights, has been recognised as having economic value that can be exploited for commercial

[623] (2016) 159 F Supp 3d ND Cal 1101 1106.
[624] (2016) 159 F Supp 3d ND Cal 1101 1115.
[625] Rabin R (2017) 328.
[626] For the conditions for law processing, see 3.3.3 and 5.3.3.2 for South Africa and the EU respectively.
[627] Solove D (2001) 1434; Purtova N (2009) 512.

https://uwcscholar.uwc.ac.za/home

gain,[628] it is argued that similar recognition ought to be given to personal data, under the appropriate circumstances, in light of current developments in commerce.

Generally, tort law's inherent shortcomings and emphasis on protecting negative rights make it an ineffective tool for addressing data protection issues.[629] Tort law neither provides the data subject with control measures to prevent unauthorised processing of personal information nor imposes data processing obligations on the data processor. In this regard, parallels may be drawn with South Africa as the law of tort in the US appears to exhibit the same shortcomings as the South African common law.[630]

4.6 AMERICAN CONSTITUTIONAL LAW

The right to privacy is not expressly mentioned in the US Constitution and must be inferred or derived from other enumerated rights by way of judicial interpretation.[631] The framers of the US Constitution feared centralised power, and therefore the idea behind the adoption of the US Constitution was to protect the American people from possible state oppression and tyranny by creating a government of limited powers.[632] The US Constitution does not place an obligation on the government to take positive steps to preserve or cultivate an individual's private sphere or allow for other fundamental rights.[633] Constitutional privacy interests restrict only government actions.[634] The duty to protect constitutional rights is not recognised in US constitutional law, which limits the extent to which constitutional rights may reach private relationships.[635] Constitutional provisions do not apply to data processing activities by the private sector,[636] which, according to Nehf, pose potentially greater harm than public sector

[628] In South Africa, it has been recognised that a person's image or likeness may be subject to commercial exploitation. See Cornelius S 'Commercial Appropriation of a Person's Image: Wells v Atoll Media (Pty) Ltd (Unreported 11961/2006) [2009] ZAWCHC 173 (9 November 2009)' (2011) 14 *PELJ* 182 194–98.

[629] Purtova N (2009) 512.

[630] See 3.3.1 above.

[631] Laudon K (1996) 94; Purtova N (2009) 512.

[632] Garry P 'Liberty through limits: The Bill of Rights as limited government provisions' (2009) 62 *SMU Law Review* 1745 1754–56; Purtova N (2009) 512; Schwartz P & Peifer K 132–33.

[633] Schwartz P & Peifer K (2017) 132–33. See also *Deshaney v Winnebago County Department of Social Services* (1989) 489 US 189 196 where the Court held that there is no obligation on the state to protect life, liberty, and property of its citizens against invasion by private persons.

[634] Purtova N (2009) 512.

[635] Chirwa D 'The horizontal application of constitutional rights in a comparative perspective' (2006) 10 *Law, Democracy & Development* 21 25; Schwartz P & Peifer K 'Transatlantic data privacy law' (2017) 106 *Georgetown Law Journal* 115 132.

[636] Solove D (2001) 1435.

https://uwcscholar.uwc.ac.za/home

processing activities.[637] Consequently, as is discussed below, US jurisprudence, insofar as it relates to constitutional rights and private conduct, is incoherent because of the lack of horizontal application. In comparison to South Africa's constitutional rights, the lack of horizontal application makes the US Constitution less able to respond to challenges brought about by technology.[638] As such, the US Constitution lacks the transformative qualities of the Constitution in addressing the needs of society insofar as it relates to data protection.

The US courts have over the years recognised constitutionally protected privacy interests in various contexts, the protection of which includes privacy in marriage,[639] reproduction,[640] birth control,[641] family relationships,[642] child rearing,[643] and education[644].[645] Nehf points out, however, that most decisions have only marginal relevance to the problem of personal data processing.[646] For the purposes of discussing US information privacy from a constitutional perspective, only certain provisions of the US Constitution have been selected, namely the due process clause of the Fourteenth Amendment,[647] the Fourth Amendment of the US Constitution and the First Amendment. Only pertinent or data processing-related aspects will be the focus of these discussions.

UNIVERSITY of the
WESTERN CAPE

4.6.1 Substantive due process clause of the Fourteenth Amendment

The US courts have used the due process clause to extend protection to rights that are not specifically enumerated in the US Constitution, such as information privacy.[648] This aspect of due process is referred to as 'substantive due process'. In this context, consideration is given

[637] Nehf J (2003) 33.

[638] See the discussion on horizontality in 3.6.2 above.

[639] *Griswold v Connecticut* (1965) 381 US 479 484–86.

[640] In *Roe v Wade* (1973) 410 US 113, the US Supreme Court granted women autonomy over bodily rights in respect of the right to abort pregnancies. This decision was subsequently overturned in *Dobbs v Jackson Women's Health Organization* (2022) 142 S.Ct. 2228.

[641] *Griswold v. Connecticut* (n 635).

[642] *Meyer v Nebraska* (1923) 262 US 390.

[643] *Washington v Glucksberg* (1997) 521 US 702.

[644] *Pierce v Society of Sisters* (1925) 268 US 510.

[645] Jacoby N 'Redefining the right to be let alone: Privacy rights and the constitutionality of technical surveillance measures in Germany and the United States' (2007) 35 *Georgia Journal of International and Comparative Law* 435 436.

[646] Nehf J (2003) 33.

[647] Section 1 of the US Constitution Amendment XIV prohibits deprivation any person's 'life, liberty, or property, without due process of law' with respect to the individual state actions. US Constitution Amendment V contains a similar provision which focuses on federal state actions.

[648] Purtova N (2009) 512.

https://uwcscholar.uwc.ac.za/home

to whether there is sufficient substantive justification to deprive an individual of his life, liberty or property.[649] In *Griswold v Connecticut* (*Griswold*),[650] the US Supreme Court applied the due process clause of the Fourteenth Amendment to invalidate a government ban on contraceptives. The Court held that even though the US Constitution does not explicitly protect the right to privacy, such a right is found in the 'penumbras' or 'zones' of freedom created by an expansive interpretation of the Bill of Rights.[651] Subsequently, in *Whalen v Roe* (*Whalen*),[652] the due process protection was extended to information privacy. The US Supreme Court recognised two different privacy interests, namely (1) a potential 'interest in avoiding disclosure of personal matters' and (2) 'independence in making certain kinds of important decisions'.[653] The first interest articulated in *Griswold* can be described as 'decisional privacy' as it relates to an individual's decisions and choices, and the second interest is often referred to as the 'constitutional right to information privacy'.[654] Therefore, the US concept of constitutional privacy encompasses a wide range of diverse legal interests, such as autonomy rights and the nondisclosure of personal data.

The significance of the due process clause means that the right to privacy is rooted in supporting fundamental liberty interests. The US concept of constitutional privacy interests relates to the extent that people have the freedom to make decisions about their lives without interference from the government.[655] The US position can be contrasted with that of South Africa and the EU, both of which specifically recognise a fundamental right to privacy that underpins human dignity. It is submitted that the US perception of privacy explains the marketplace discourse that has been adopted around personal data.[656] The aim of privacy rights is to ensure that individuals have the freedom to trade and exchange their personal data for benefits. Therefore, it may be argued that privacy rights only become relevant if the government enacts laws that limit the exercise of fundamental liberty interests. The consideration of dignity generally is not a significant factor in the ensuing commodification of personal data. As such, it is

[649] Chemerinsky E 'Substantive due process' (1999) 15 *Touro Law Review* 1501 1501. Substantive due process is distinguished from procedural due process, which prohibits the government from depriving an individual of a protected interest without following proper procedures.
[650] (1965) 381 US 479.
[651] (1965) 381 US 479 484.
[652] (1977) 429 US 589.
[653] (1977) 429 US 589 599–600. See also Cate F & Cate B 'The Supreme Court and information privacy' (2012) 2 *International Data Privacy Law* 255 258.
[654] Cate F & Cate B (2012) 256; Solove D (2016) 23–4.
[655] *Planned Parenthood of Southeastern Pennsylvania et al v Casey, Governor of Pennsylvania et al* (1992) 505 US 833 851.
[656] See 4.2 above.

https://uwcscholar.uwc.ac.za/home

inconsequential if humans are viewed as mere objects since they stand to benefit as consumers from innovation and technological developments. On the other hand, dignity plays a prominent role in determining how the commodification of personal data in seen in the EU context.[657] This will also be of relevance to the South African context since South Africa also follows a dignity-based approach in dealing with privacy and data processing issues.[658]

It is also submitted that the ineffectiveness of the right to privacy stems from the uncertainty surrounding the precise nature of the US constitutional right to privacy. Fourteenth Amendment jurisprudence is characterised by the failure of the US Supreme Court to clarify the exact nature and limits of the constitutional right to privacy. In most instances, the US Supreme Court has simply assumed the existence of such a right without providing much guidance as to its meaning.[659] This would effectively render the courts incapable of achieving a fair balance between individual privacy interests and government action. The uncertainty has also resulted in variations in interpretations by the lower courts.[660] Some lower courts recognise a constitutional right to information privacy, but only when it implicates a fundamental right or one implicit in ordered liberty.[661] This narrow interpretation limits protection to specific categories of personal information, resulting in insufficient protection for most personal data under government control.[662] Consequently, in US constitutional law, information privacy remains a hypothetical right.[663]

Purtova comments that the significance and use of substantive due process for the purposes of data protection are limited since it protects only information privacy, understood as the non-disclosure of personal information.[664] The constitutional right to information privacy is accordingly premised on the 'right to be left alone' principle discussed above.[665] Consequently,

---

[657] See 5.2 below.

[658] See 3.3.3 above.

[659] Solove D (2001) 1437; Gilbert H 'Minors' Constitutional Right to Informational Privacy' (2007) 74 *University of Chicago Law Review* 1375 1381; Gorkin R 'The Constitutional Right To Informational Privacy: NASA v Nelson' (2010) 6 *Duke Journal of Constitutional Law & Public Policy Sidebar* 1 5; Azarchs T 'Informational Privacy: Lessons from Across the Atlantic' (2014) 16 *Journal of Constitutional Law* 805 814; Schwartz P & Peifer K (2017) 133; Pittman L 'The Elusive Constitutional Right to Informational Privacy' (2018) 19 *Nevada Law Journal* 135 157; *Nixon v Administrator of General Services* (1977) 433 (US) 425 455; *National Aeronautics and Space Administration v Nelson* (2011) 131 S.Ct 746 751.

[660] Gilbert H (2017) 1381.

[661] Gilbert H (2017) 1382; *J P v DeSanti* (1981) 653 F2d 6th Cir 1080 1088; *Kallstrom v City of Columbus* (1998) 136 F3d 6th Cir 1055 1062.

[662] Schwartz P (1999) 828–29.

[663] Azarchs T (2014) 813.

[664] Purtova N (2009) 513 See also Solove D (2001) 1436.

[665] See 4.3 above. See also Pittman L (2018) 141.

https://uwcscholar.uwc.ac.za/home

due process protection is constrained by the privacy-as-secrecy paradigm, namely protecting one's hidden world.[666] Moreover, the uncertainty as to the reach and scope of the right to information privacy means that the protection afforded to individuals may be limited to only a few types of personal information.[667] Most decisions concern either a breach of confidentiality or the disclosure of highly private facts, such as information relating to sexual practices or medical conditions.[668] Medical records may be protected under the constitutional information privacy,[669] on the other hand, public records, including arrest or conviction records, are not.[670] Only information deemed highly personal, non-public, or confidential is protected, resulting in many types of other personal information not qualifying for protection.[671]

It is submitted that due to the limited types of information that qualify for protection, the Fourteenth Amendment fails to provide adequate data protection. Individuals require protection regardless of whether the information concerned can be characterised as confidential or highly sensitive. This private/public dichotomy continues to play an important role in shaping US privacy law. Given the prevalence of profiling based on publicly accessible information and the willingness of individuals to exchange personal information for various reasons, it seems unlikely that individuals will obtain adequate protection under the Fourteenth Amendment.

UNIVERSITY of the
WESTERN CAPE

4.6.2 The Fourth Amendment

The Fourth Amendment of the US Constitution is also a primary source for the recognition of a constitutional right to privacy.[672] The Fourth Amendment provides that '[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches

---

666 Solove D (2001) 1437. This understanding of privacy is also prominent in the South African context.

667 Schwartz P (1999) 829; Purtova N (2009) 513.

668 Nehf J (2003) 34.

669 In *United States v Westinghouse Electric Corporation* (1980) 638 F2d 3d Cir 570 580–81, the court held that the request for employee medical records to investigate work related hazards justified a minimal intrusion into the privacy of the employees. The Court held further that affected employees should be given prior notice and the opportunity to object to such investigation. In *Doe v Borough of Barrington* (1990) 729 F Supp DNJ 376 385, the court held that an individual's rights to privacy are infringed where the state discloses that such a person has AIDS without a compelling interest for doing so.

670 In *Russel v Gregoire* (1997) 124 F3d 9th Cir 1079 1094, the court held that a law requiring the public be informed of sex offenders does not infringe privacy since the arrest and conviction records are available publicly. In *Cline v Rogers* (1996) 87 F3d 6th Cir 176 179, the court stated that a public record cannot be protected.

671 Nehf J (2003) 35.

672 Cate F & Litan R 'Constitutional issues in information privacy' (2002) 9 *Michigan Telecommunications and Technology Law Review* 35 42.

https://uwcscholar.uwc.ac.za/home

and seizures, shall not be violated…'. The roots of the Fourth Amendment may be traced back to a significant popular outcry against the British government's use of arbitrary and intrusive searches to, among other things, enforce tax laws and suppress dissent.[673] Consequently, the purpose of the Fourth Amendment is not to preclude the government from conducting searches but rather to protect an individual's privacy and dignity against arbitrary and unlawful searches and seizures.[674] The Fourth Amendment limits the power of the government, both federal and state, to collect personal data through a search or seizure.[675]

Although the Fourth Amendment serves as a general framing device for a great deal of privacy discourse in the US, it is limited to only privacy interests that implicate nondisclosure and autonomy rights against the government. The limited reach of the Fourth Amendment and the US Constitution as a whole is demonstrated by the state action doctrine.[676] The implication of the state action doctrine means that the US Constitution does not apply when an activity protected as an individual right is interfered with by private action, regardless of the extent of the interference. In other words, the US Constitution does not apply to horizontal relationships.

This is problematic in view of the accretion of power by the private sector and potential data processing infringements concerning individuals.[677] Although there is an exception to the state action doctrine that allows the US Constitution to be enforced against a private entity when that entity exercises a power traditionally and exclusively reserved for the state,[678] it is argued that this exception will have limited application when it concerns the commodification of personal data because the private sector is typically motivated by their own interests to collect and process personal data. Considering that the purpose of the state action doctrine is to limit government intrusion into the private sphere of individuals, the lack of horizontal effect may actually prove counterintuitive due to the significant influence and power that the private sector wields and their ability to invade individuals' privacy.[679] However, the US seems to have embraced the attitude that whatever is beneficial for the economy must also be beneficial for

[673] Price M 'Rethinking privacy: Fourth Amendment "papers" and the third-party doctrine' (2016) 8 *Journal of National Security Law & Policy* 247 250–58.
[674] Cate F & Cate B (2012) 261.
[675] Purtova N (2009) 513.
[676] For an explanation of the state action doctrine, see Meacham M 'The perfect storm: How narrowing of the state action doctrine, inconsistency in Fourth Amendment caselaw, and advancing security technologies converge to erode our privacy rights' (2019) 55 *Idaho Law Review* 309 318–19.
[677] See 3.6.2 above.
[678] Meacham M (2019) 319–20.
[679] See 2.3.4 above for examples of how information may be used to the detriment of the individual.

https://uwcscholar.uwc.ac.za/home

society, thus prioritising innovation over the protection of individuals' privacy. It is therefore no surprise that the US relies heavily on industry self-regulation for consumer privacy.[680]

This raises an interesting question as to whether the horizontal application of fundamental rights will place the individual in a better position in light of the commodification of personal information. The next chapter delves into this aspect, which is also relevant to the South African context because the Constitution expressly commits to horizontality.[681]

4.6.3 The First Amendment

In the US, a preference for the free flow of information means that the most significant constitutional safeguards concern the free flow of information rather than privacy.[682] The notion of a free flow of information is embodied in various constitutional provisions pertaining to freedom of expression,[683] copyright[684] and the delivery of mail and news.[685] Privacy protection entails interfering with information flows and other constitutional values enshrined in the First Amendment, such as free expression.[686] Consequently, courts in the US have faced a continuous and persistent challenge to balance the competing values and interests represented by an individual's right to privacy and the right of society to information.[687] In *Florida Star v B.J.F. (Florida Star)*,[688] the Court held that the First Amendment precluded a newspaper from being held liable under a state law for publishing the name of a rape victim lawfully obtained from a publicly released police report.[689] *Florida Star* suggests that the privacy interests of an individual wishing to protect their privacy interests may not be sufficiently compelling to justify a ban against publication in circumstances where such information is lawfully obtained by the press. When information is true and lawfully obtained, the US Supreme Court favours first amendment interests such as free speech over privacy rights.[690]

---

[680] See 4.7 below.
[681] See 3.6.2 above.
[682] Schwartz P & Peifer K (2017) 134. See also 4.2 above.
[683] US Constitution, Amendment. I.
[684] US Constitution, Amendment I, s 8, clause 8.
[685] US Constitution, Amendment I, s 8, clause 7.
[686] Cate F 'Principles of Internet Privacy' (2000) 32 *Connecticut Law Review* 877 886–87.
[687] McNulty P (2001) 94.
[688] (1989) 491 US 524.
[689] (1989) 49 US 524 541.
[690] Murphy R (1996) 2392; Solove D (2001) 1456; Cate F & Cate B (2012) 260.

https://uwcscholar.uwc.ac.za/home

On the face of it, this does not appear to be any different from any other jurisdiction where the need to protect privacy rights must be balanced against conflicting rights and interests. In the South African context, it was mentioned that the right to privacy is not absolute.[691] But whereas in South Africa the values of dignity, equality and freedom must inform constitutional adjudication, this is not the case in the US. Consequently, rights such as privacy that are more closely linked with the values of dignity, equality and freedom tend to prevail over economic rights in the South African setting.[692] In the US, first amendment rights like free speech on matters of public interest have been elevated above other interests such as privacy protection.[693] As a result, the US generally displays indifference for privacy as a matter that requires protection from the private sector.[694]

This creates an enabling environment for the private sector to collect and exploit personal data. Companies' positions are further bolstered by the fact that neither the due process clause nor the Fourth Amendment apply. In *Sorrell v IMS Health Inc* (*Sorrell*),[695] the US Supreme Court had to revisit the balance between First Amendment protection and data protection laws. *Sorrell* involved the mining of large databases and the sale of prescription drug user data for marketing prescription drugs. The Court considered a challenge to a Vermont law that restricted the sale, disclosure and use of personal data in pharmacy and related records for use in marketing or promoting prescription drugs unless the consent of the prescribing physician or doctor was obtained.[696] The law was aimed at 'protecting medical privacy, including physician confidentiality, avoidance of harassment, and the integrity of the doctor-patient relationship'.[697] However, the law permitted that same information to be sold to academic researchers without the consent of the prescribing physician.[698] The US Supreme Court held that the Vermont law violated the First Amendment as it discriminated against pharmaceutical companies by prohibiting the commercial use of the data while permitting non-commercial

[691] See 3.6.2 above.
[692] See 3.6.2 above.
[693] *Snyder v Phelps* (2011) 562 US 443 451–52.
[694] In *Snyder v Phelps* (2011) 562 US 443 452 the court held '… where matters of purely private significance are at issue, First Amendment protections are often less rigorous. … That is because restricting speech on purely private matters does not implicate the same constitutional concerns as limiting speech on matters of public interest'.
[695] (2011) 564 US 552.
[696] (2011) 564 US 552 557–59.
[697] (2011) 564 US 552 572.
[698] (2011) 564 US 552 562–63.

https://uwcscholar.uwc.ac.za/home

use.[699] Moreover, the law was limited in its ability to protect the asserted privacy interests since the prescriber data was widely available without requiring consent.[700]

Bhagwat notes that a fundamental question avoided by the Court in *Sorrell* was whether a flat restriction on data disclosure potentially constitutes an infringement of the First Amendment given the broad range of rules, existing and proposed, that seek to control the disclosure of personal information in order to protect privacy.[701] It is suggested that any restrictions on speech imposed by federal data protection regulations would be subject to stringent review by a reviewing court.[702] Schwartz and Peifer state, with merit, that: 'The First Amendment is likely to be an increasingly fertile source of rights for data processors… .'[703]

It is submitted that the First Amendment is a cornerstone of US democracy and guarantees many of the freedoms that are fundamental to US society. The First Amendment explicitly guarantees the unrestricted exchange of knowledge, which enables innovation and advancement. In contrast, the US Constitution does not contain any express rights to privacy. An implied right to privacy has been derived from the penumbras of other explicitly stated constitutional protections. The regulation of data processing gives rise to First Amendment considerations, necessitating the courts to find a middle ground between safeguarding privacy and upholding freedom of speech. It is submitted that, given the US approach to data protection, the default position is to prioritize the free flow of information and ideas. This is consistent with an 'opt-out' approach to data protection.[704]

4.7 STATUTORY DATA PROTECTION LAWS

Given the inherent limitations of tort law and constitutional law, various statutory laws have been enacted to provide personal data protection to individuals.[705] These statutory laws are framed to promote the individual as a 'privacy consumer'. This positions the individual as a participant in a commercial relationship.[706] US data protection law takes the form of a

[699] (2011) 564 US 552 572–73.
[700] (2011) 564 US 552 573.
[701] Bhagwat A 'Sorrell v. IMS Health: Details, detailing, and the death of privacy' (2012) 36 *Vermont Law Review* 855 855–56.
[702] Congressional Research Service *Data Protection Law: An Overview* (2019) 70.
[703] Schwartz P & Peifer K (2017) 134.
[704] See generally 4.7.2 below.
[705] Congressional Research Service *Data Protection Law: An Overview* (2019) 7.
[706] Schwartz P & Peifer K (2017) 121.

https://uwcscholar.uwc.ac.za/home

'patchwork of uneven, inconsistent, and often irrational' statutes and regulations at both the federal and state level.[707] The legislative process to protect data privacy is initiated as and when data privacy issues become problematic and there is evidence of abusive data practices.[708] Laws and regulations, at both the federal and state levels, are usually only adopted in response to specific industry violations.[709] The failure of US policymakers to adopt comprehensive privacy regimes partially explains this sectoral approach.[710] The following sections examine selected aspects of statutory protection that are relevant for discussing data processing problems.

4.7.1 Code of Fair Information Practices

Due to the ever-increasing computerisation of information and repositories of personal data, the US federal government responded to increased public concerns pertaining to automated data systems.[711] In 1973, the US Department of Health Education and Welfare (HEW) exhaustively investigated the concerns and made recommendations in a report titled, 'Records, Computers, and the Rights of Citizens'.[712] The HEW report noted:[713]

> '[A]n individual must increasingly give information about himself to large and relatively faceless institutions, for handling and use by strangers—unknown, unseen, and, all too frequently, unresponsive. Sometimes the individual does not even know that an organization maintains a record about him. Often he may not see it, much less contest its accuracy, control its dissemination, or challenge its use by others.'

The HEW report recommended the adoption of a Code of Fair Information Practices (Code) based on five principles:[714]

- a prohibition on the use of secret personal data record-keeping systems;

[707] Bergelson V (2003) 391.
[708] Schwartz P & Peifer K (2017) 136.
[709] Bergelson V (2003) 392.
[710] Rotenberg M 'Fair information practices and the architecture of privacy (What Larry doesn't get)' (2001) 2001 *Stanford Technology Law Review* 1 10.
[711] Purtova N (2009) 513; Ohm P 'Broken promises of privacy: Responding to the surprising failure of anonymization' (2010) 57 *University of California Law Review* 1701 1733.
[712] US Department of Health, Education and Welfare *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (1973).
[713] US Department of Health, Education and Welfare (1973) 29.
[714] US Department of Health, Education and Welfare (1973) 41–2.

https://uwcscholar.uwc.ac.za/home

- an individual must have the ability to find out what personal data relating to him has been collected and how it was used;
- an individual must be able to prevent personal information collected for a specific purpose being used for a purpose other than the one for which it was collected without consent;
- an individual should be entitled to rectify or amend any personal data records about him; and
- any organisation that processes personal data must assure the reliability of and take reasonable precautions to prevent the misuse of the data.

Ohm comments that a significant change to privacy law brought about by the adoption of these principles (FIPs of FIPPs)[715] contained in the Code was that rights of privacy were no longer focussed solely on redressing past wrongs as was the case with privacy torts.[716] FIPs aspired to create an environment in which the privacy of individuals would be respected while simultaneously promoting the flow of information in an increasingly technology-dependent, global society.[717] A key notion underpinning the FIPs is that individuals have an interest in records containing information about themselves, even when such records are created by third parties.[718] As such, it recognises the individual's right to information privacy.[719]

Rotenberg observes that the FIPs have 'played a significant role in framing privacy laws in the United States, and these basic principles have also contributed to the development of privacy laws around the world including the development of important international guidelines for privacy protection.'[720] The FIPs were adopted by the OECD in its Guidelines on the Protection of Privacy and Transborder flows of Personal Data and by the Council of Europe in the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[721] Purtova points out, however, that a fundamental shortcoming of the Code was that it

[715] Fair Information Practices (FIPs) and Fair Information Practice Principles (FIPPs) are used interchangeably in this study. See also Solove D & Hartzog W 'The FTC and the new common law of privacy' (2014) 114 *Columbia Law Review* 583 592.
[716] Ohm P (2010) 1734.
[717] Cate F 'The failure of fair information practice principles' in Winn J (ed) *Consumer Protection in the Age of the Information Economy* (2006) 343.
[718] Laudon K (1996) 96.
[719] Purtova N (2009) 514.
[720] Rotenberg M (2001) 15. FIPs have influenced the development of data protection frameworks such as the GDPR and POPIA.
[721] Hartzog W 'The inadequate, invaluable fair information practices' (2017) 76 *Maryland Law Review* 952 957–58.

https://uwcscholar.uwc.ac.za/home

was not directly binding and therefore its significance was diminished in the course of implementation.[722] Moreover, the Code did not apply to all sectors, nor did it provide for adequate enforcement and oversight.[723]

Despite the shortcomings, FIPs have evolved to provide for new data protection rights such as the 'right to portability'[724] and 'right to be forgotten'.[725] For the purposes of this dissertation, it is important to note that the FIPs model of privacy regulation or data protection has provided the foundational elements for a property-based rights-and-remedies scheme for personal data. This model facilitates the transfer of personal data while incorporating property-like rights and remedies for the purposes of providing privacy protection to individuals. The next chapter will delve deeper into this aspect within the framework of the GDPR.[726] Compared to POPIA and the GDPR, sectoral legislation in the US has incorporated FIPs to a lesser extent. However, it is submitted that the FIPs offer a framework that aligns with how personal data is treated in the US. In other words, it facilitates the exchange of personal data.

4.7.2 Federal Trade Commission

UNIVERSITY of the WESTERN CAPE

The FTC, a US federal agency, has adopted a version of the FIPPs that is narrower in scope, shorter, and less complete than the original principles contained in the Code.[727] Solove and Hartzog state that FTC privacy jurisprudence is 'the broadest and most influential regulating force on information privacy in the United States – more so than nearly any privacy statute or common law tort.'[728] This is primarily due to the sectoral approach to privacy regulation, which leaves many areas unregulated at a federal level, resulting in the FTC being the single most dominant agency that enforces and deals with privacy.[729] Zarsky comments that the FTC acts as the de facto US privacy regulator.[730]

[722] Purtova N (2009) 514.
[723] Rotenberg M (2001) 16; Cate F (2006) 348.
[724] See 5.4.1.2.3 below.
[725] See 5.4.1.3 below.
[726] See 5.4.1 below.
[727] Gellman R *Fair Information Practices: A Basic History* 2019 22–3.
[728] Solove D & Hartzog W (2014) 585–87.
[729] Solove D & Hartzog W (2014) 588.
[730] Zarsky T (2015) 158.

https://uwcscholar.uwc.ac.za/home

The FTC derives its authority to deal with privacy matters from s 45(a) of the FTC Act,[731] which seeks to prohibit a broad range of unscrupulous or misleading practices that are harmful to consumers.[732] In contrast, data protection legislation in the EU and South Africa establishes an independent supervisory authority to specifically ensure the lawful processing of personal data.[733] It is submitted that the legislated powers of such an authority, as opposed to the putative authority of the FTC, can better ensure greater compliance with data protection laws.

As many companies have privacy policies, the FTC can institute legal action against a company for breaching a promise in its privacy policy or for any deceptive or unfair act or practice. [734] Privacy policies are largely voluntary and self-regulatory measures implemented by companies to promote consumer trust and obviate the need for government regulation.[735] The FTC supports these self-regulatory efforts.[736] In 1998, the FTC submitted a report to Congress that examined the information practices of commercial sites on the Internet and efforts by industry to implement self-regulatory programmes to promote consumer trust and protect the online privacy of consumers.[737] The FTC identified the following five core FIPPs: [738]

- a consumer must be given notice of an entity's information practices before his personal information may be collected in order for the consumer to make an informed choice about whether and to what extent he will disclose such information;

- the choice/consent principle relates to consumer choice or consent regarding how personal information that was collected may be used including secondary uses;

- an individual's must be able to access and review data about himself in order to correct errors thereby ensuring its accuracy and completeness;

---

[731] Federal Trade Commission Act 1914.

[732] Congressional Research Service *Data Protection Law: An Overview* (2019) 30.

[733] See s 39 of POPIA and art 51 of the GDPR in this regard.

[734] Solove D & Hartzog W (2014) 588.

[735] Solove D & Hartzog W (2014) 593–94.

[736] FTC *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers* (2012) 11–4. See also Van Hoboken J 'From collection to use in privacy regulation? A forward-looking comparison of European and US frameworks for personal data processing' in Van der Sloot B, Broeders D & Schrijvers E (eds) *Exploring the Boundaries of Big Data* (2016) 244.

[737] FTC *Privacy Online: A Report to Congress* (1998) available at *https://www.ftc.gov/sites/default/files/documents/reports/privacy–online–report–congress/priv–23a.pdf* (accessed 8 December 2020).

[738] FTC *Privacy Online: A Report to Congress* (1998) 7–11.

https://uwcscholar.uwc.ac.za/home

- data collectors must take reasonable steps to protect information and ensure its accuracy and integrity; and

- privacy principles will only be effective if there are sufficient enforcement mechanisms to hold data collectors accountable.

The FTC approved a second, watered-down version of the FIPPs in 2000, which removed enforcement as a principle.[739] As only two of the core principles have implications for data collection and use, namely 'notice' and 'choice', Gellman states that these two principles are sometimes presented as an implementation of FIPPs.[740] However, notices are often complicated and difficult to understand, while individuals are presented with few meaningful opportunities to exercise choice.[741] Van Hoboken comments the FTC's notice and choice regime of privacy self-regulation has largely ignored substantive aspects concerning collection limitation and legitimate data processing.[742] Hartzog argues, correctly in my view, that the FIPPs-based data protection regimes are nothing more than procedural and formalistic exercises designed to extract consent and provide individuals with the illusion of enhanced privacy.[743]

It is submitted that the approach taken by the FTC to reduce notice and consent to a mere formality, a checkbox that consumers must select to obtain a desired product or service, is indicative of the importance attached to unimpeded information flow and the market economy rather than data protection.[744] This inevitably creates an environment that treats personal data as a commodity. On the other hand, the European Data Protection Supervisor (EDPS) bases its approach on safeguarding dignity to prevent the perception of personal data as a commodity.[745] Ostensibly, it would be reasonable to argue that the South African Information Regulator could follow a similar approach to that of the EDPS, given the place that dignity occupies.[746] However, the chapters that follow will delve further into this aspect.

The FTC's notice and choice regime is criticised for being ineffective, overburdening individuals with lengthy, vague privacy policies, and implementing a weak form of consent that

---

[739] FTC *Privacy Online: Fair Information Practices in the Electronic Marketplace* (2000) 4.
[740] Gellman R (2019) 23.
[741] Cate F (2006) 343.
[742] Van Hoboken J *Exploring the Boundaries of Big Data* (2016) 244.
[743] Hartzog W (2017) 965.
[744] See Cate F (2006) 358. See also 4.2 above.
[745] EDPB & EDPS *Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)* (2022) para 15.
[746] See 3.3.3 above.

https://uwcscholar.uwc.ac.za/home

is satisfied by 'opt-outs' or 'take it or leave it' options.[747] An opt-out approach means that companies merely have to notify consumers of their information practices and provide them with an option to opt out of using the service. Should consumers fail to opt out, then the companies are free to use the information in accordance with their information practices. This weak form of consent encourages the free flow of information, supporting Aretz and Strandburg's argument that, from a US perspective, innovation will be more beneficial than privacy.[748] Unlike rights-based regimes like South Africa and the EU, the expectation is that the individual has the primary responsibility for safeguarding privacy by choosing whether to participate in or abstain from personal data exchanges. The FTC's implementation of consent contrasts with the higher standard for consent required in terms of POPIA and the GDPR.[749] Both POPIA and the GDPR implement an opt-in mechanism that requires consent to be freely given, specific, and informed. This imposes a burden of proof on the data processor to demonstrate that the data subject's consent is valid. The FTC recognises that self-regulatory efforts in the US have fallen short of expectations by failing to provide consumers with adequate data protection.[750]

UNIVERSITY of the
WESTERN CAPE

4.7.3 Selected federal statutes

The US uses a sectoral approach to mitigate harms in specific sectors, which means that different industries are subject to different laws to regulate personal data. For example, the Financial Services Modernization Act,[751] more commonly known as the Gramm-Leach-Bliley Act (GLBA), is a federal law that imposes data protection obligations on companies offering financial products and services to consumers. Another example is the Health Insurance Portability and Accountability Act (HIPAA),[752] a federal law enacted to facilitate health insurance transferability and the transfer of private health information, such as medical records, between entities. Unlike South Africa and the EU, which have extensive and all-encompassing data protection laws that provide a reasonably wide-ranging definition of personal data, the

[747] Van Hoboken J *Exploring the Boundaries of Big Data* (2016) 245.
[748] See 4.2 above.
[749] See s 11(1)(a) of POPIA and article 6(1) of the GDPR.
[750] FTC *Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers* (2012) 11–2.
[751] Financial Services Modernization Act of 1999.
[752] Health Insurance Portability and Accountability Act of 1996.

https://uwcscholar.uwc.ac.za/home

definition of personal data in the US varies depending on the specific industry and applicable statute.

While these and other sector-specific laws seek to mitigate the misuse of personal data, such aims are generally subservient to the need to ensure the transferability of such data. For example, the GLBA permits financial institutions to share individuals' personal data with third parties provided such individuals have the right to opt out.[753] On the other hand, HIPAA provide more opportunities for consumer opt-in consent concerning health information.[754] Therefore, health practitioners and healthcare providers that are subject to HIPAA may not disclose protected health information unless the individual authorises such disclosure in writing or as provided for in HIPAA.[755]

Generally, these sector-specific laws offer weak privacy protection to individuals.[756] The laws are not specifically designed to safeguard privacy. Instead, the laws are enacted to implement limits as to how personal data may be used or disclosed. This illustrates that the primary concern regarding the most important constitutional protections for information in the US is the unrestricted exchange of information, rather than privacy.

UNIVERSITY of the
WESTERN CAPE

4.7.4 California Consumer Privacy Act (CCPA)

The CCPA is a state law passed by the California legislature to enhance consumer privacy rights and afford individuals more control over the personal information that businesses collect about them. It is often referred to as the US version of the GDPR and is considered to provide the strongest consumer protection in the US.[757] The CCPA differs from the federal sector-specific legislation in that it applies to any company that collects personal information about California

[753] Section 502(b)(1)(A)–(C), Financial Services Modernization Act of 1999.

[754] Cate F *Consumer Protection in the Age of the Information Economy* (2006) 359.

[755] 45 CFR s 164.520(a)–(b).

[756] Anglim J, Kirtley J & Nobahar G (eds) *Privacy Rights in the Digital Age* (2015) 213; McKinstry C 'The HIPAA privacy rule: Flawed privacy exposed when compared with the European Union's General Data Protection Regulation' (2018) *Journal of Health Care Finance* 1 2.

[757] Viljoen S 'The promise and pitfalls of the California Consumer Privacy Act' undated available at *https://www.dli.tech.cornell.edu/post/the–promise–and–pitfalls–of–the–california–consumer–privacy–act* (accessed 15 December 2020). Several other US states are expected to follow California in implementing GDPR-influenced statutes in 2023. For more information see Bellamy F 'US Data privacy laws to enter new era in 2023' *Reuters* 12 January 2023 available at *https://www.reuters.com/legal/legalindustry/us–data–privacy–laws–enter–new–era–2023–2023–01–12/* (accessed 4 August 2023).

https://uwcscholar.uwc.ac.za/home

residents for commercial purposes, provided certain thresholds are met.[758] The CCPA broadly defines personal information as 'information that identifies, relates to, describes, or is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household'.[759] Unlike federal legislation, the CCPA regulates all personal information irrespective of the source of the information but creates exceptions in respect of publicly available information and certain types of personal information already regulated by existing federal legislation, such as the HIPAA[760] and GLBA.[761]

The rights under the CCPA are, to a certain extent, inspired by the GDPR. First, the 'right to know' requires that businesses inform consumers, prior to the collection of personal information, as to the categories of personal information to be collected and the purposes to which the information will be put.[762] Secondly, a consumer has the right, in certain circumstances, to request that a business delete any personal information that it has collected from the consumer.[763] Thirdly, the CCPA provides rights regarding portability should the consumer wish to move information from one entity to another.[764] Unlike the GDPR, the CCPA makes provision for a consumer's right to opt out in connection with the sale of personal data by a business to a third party.[765] Moreover, the proposed CCPA regulations make provision for businesses to offer financial incentives to individuals in exchange for their personal information.[766] The use of such language seems to confirm that personal information is a commodity that can be traded or sold and vests individuals with ownership rights in their personal information. De Rosario postulates, correctly in my view, that the CCPA creates property interests in personal information while employing a property regime to regulate the processing of personal information.[767] Similarly, Masciandaro states that state legislatures are

[758] Sections 1798.140(c)(1)–1798.140(c)(2), CCPA. These thresholds include the application of the CCPA to only for-profit companies which do business in the state of California that have a revenue of US$25 million; buy, receive or sell the personal information of fifty thousand or more California residents, households or devices; or generate 50 per cent or more of their annual revenue from selling the personal information of California residents.

[759] Section 1798.140(o)(1), CCPA.

[760] Section 1798.145(c)(1)(A), CCPA.

[761] Section 1798.145(e), CCPA.

[762] Section 1798.100(b), CCPA.

[763] Section 1798.105, CCPA.

[764] Section 1798.100(d), CCPA.

[765] Section 1798.120, CCPA.

[766] Section 7016(b)(1–5), Proposed California Consumer Privacy Act Regulations.

[767] Del Rosario L 'On the propertization of data and the harmonization imperative' (2022) 90 *Fordham Law Review* 1699 1720–23.

https://uwcscholar.uwc.ac.za/home

extending property rights to personal information under the guise of privacy.[768] It is submitted that although the CCPA attempts to break away from the traditional notice and consent model that is so prevalent in the US by affording consumers greater control over their personal data, the overarching focus that underpins the CCPA remains the promotion of innovation and economic prosperity. In this sense, it is argued that the direction of the CCPA is no different from current federal sectoral laws that treat personal data as a commodity.

A notable weakness of the CCPA is that it applies to only for-profit organisations that process personal data of Californian residents. Another significant shortcoming concerns the definition of personal information which specifically excludes publicly available information.[769] As was discussed in chapter two, big data technologies enable inferences and predictions to be made about individuals by collecting and analysing publicly available information, thereby invading privacy and undermining individual autonomy.[770]

4.8 REMARKS

US privacy laws, specifically tort and constitutional law, subscribe to the privacy-as-secrecy paradigm. Murphy considers the preference for the free flow of information as enshrined in the First Amendment over vaguely defined privacy interests as a reason for tort failing as a tool for protecting privacy.[771] Tort is handicapped because it provides protection in the form of negative rights and fails to provide the individual with any control over the processing of his personal data. US constitutional remedies are limited as they do not have horizontal reach and therefore do not regulate private relationships.[772] A reluctance to properly define the contours of the constitutional right to privacy has caused US jurisprudence to be significantly incoherent and inconsistent. A number of federal statutes adopted since the 1970s have introduced positive data protection rights; however, these statutes are directed primarily at the public sector, leaving data processing by the private sector mostly unregulated. As a result, the US adopts a sectoral

[768] Masciandaro A 'Cleaning-up after carpenter: Personal data as property under the Fourth Amendment' (2021) 51 *Seton Hall Law Review* 1241 1259–60.

[769] Section 1798.140(o)(2), CCPA. Masciandaro A (2021) 1269 points out that the exclusion of publicly available information is also consistent with the view that personal information is treated as property for purposes of the Fourth Amendment, as individuals cannot have any expectations of privacy in respect of public information.

[770] See 2.3.3 above.

[771] Murphy R (1996) 2392; Scholz L 'Privacy as quasi-property' (2016) 101 *Iowa Law Rev* 1113 1113.

[772] This is especially relevant in the data economy since the private sector is responsible for processing large volumes of personal data. See 3.6.2 for a discussion on horizontality in the South African context.

https://uwcscholar.uwc.ac.za/home

approach to regulating the processing of specific types of personal data, leaving the FTC to monitor and regulate many other forms of information practices, which it does from a consumer rights perspective rather than a privacy perspective. Sectoral laws seek to facilitate the free flow of information and, consequently, offer individuals limited control over the processing of their personal data while imposing relatively weak obligations on companies wishing to process personal data. The perceived weaknesses in the existing legal mechanisms have led to calls for the creation of personal data property rights as an alternative solution in the US. The next section will delve into this aspect.

4.9 PROPERTY RULES FOR PERSONAL INFORMATION

The commodification of personal information is an inevitable consequence of a marketplace discourse that prioritises the free flow of information over privacy in favour of economic growth.[773] Businesses leverage the economic value of personal information in their business models, and individuals use their personal information as a means of exchange or payment.[774] The same personal information may be transferred to others for use in other contexts.[775] To facilitate the personal information trade, the US anchors its data protection law in the marketplace, where the individual, as a consumer, participates in free exchanges involving his personal information.[776] The US data protection regime, however, offers individuals little control over their personal information, especially when it concerns data processing in the private sector.[777] Instead, the US approach to data protection and privacy relies on building consumer trust in the digital economy and instilling the belief that processing personal data will not adversely affect the individual.[778] However, as Del Rosario correctly points out, 'trust cannot prevent harm'.[779] Trust does not place individuals in a position where they can proactively try and minimise any potential harms that may result from the processing of personal information.

---

[773] See 4.2 above.

[774] Schwartz P 'Property, privacy and personal data' (2004) 117 *Harvard Law Review* 2055 2056–57. See also 1.1 above.

[775] See 1.1 above.

[776] Schwartz P & Peifer K (2017) 132. See also 4.2 above.

[777] Purtova N (2009) 514. See also Lynskey O (2015) 233. The shortcomings of US data protection system have been highlighted in 4.8 above.

[778] White House (2014) 9–10.

[779] Del Rosario L (2022) 1699 1712. The ultimate goals of US data protection are to promote innovation and human flourishing. See 4.2 above.

https://uwcscholar.uwc.ac.za/home

Introducing property rights in personal data is suggested as a possible solution for ensuring individuals can exercise greater control over their personal data and creating a better system of data protection in the US.[780] The subsections that follow examine the different economic arguments for implementing property rights in personal information.

4.9.1 Economic arguments for Propertisation

As the emphasis of data protection in the US is to police the fairness of the exchange of personal data in the marketplace, commodified personal data interests are convenient subjects for market-based models as opposed to government regulation.[781] An economic analysis of law conceives property as a tool to facilitate market exchange.[782] According to Solove, the market discourse focuses on who should own certain kinds of information and the appropriate contractual rules that should be in place to regulate the trading of personal information.[783] By approaching privacy in terms of property rights to assign entitlements instrumentally, it is claimed the market will achieve optimal privacy by balancing the value of personal information to a company against the value of the information to the individual and the larger social value of data protection. [784] Several property rules have been proposed to efficiently allocate default entitlements and regulate the use of resources in the market. These rules are briefly described below.

4.9.2 Overview of property rules

Some scholars assume that personal information is property, and therefore the question that must be dealt with concerns which party owns the property rights to such information: the individual to whom the information pertains, the data collector, or both.[785] This rationale is based on the idea that an unrestricted flow of information is necessary for improved levels of

[780] Schwartz P (2004) 2055 2056–68; Purtova N (2009) 514–15; Del Rosario L (2022) 1704; Baron J 'Property as control: The case of information' (2012) 18 *Michigan Telecommunications and Technology Law Review* 367 380–81.
[781] Litman J (2000) 1289.
[782] Purtova N (2009) 515.
[783] Solove D (2001) 1446.
[784] Solove D (2001) 1446–47.
[785] Murphy R (1996) 2383–84; Kang J 'Information Privacy in Cyberspace Transactions' (1998) 50 *Stanford Law Review* 1193 1246.

https://uwcscholar.uwc.ac.za/home

economic exchange.[786] The issue of market efficiency prompts the inquiry of whether it is more advantageous for individuals to possess their personal data or for it to be assigned to another party.[787] In this instance, the answer is dependent on what would be most optimal for the market.

Other scholars, like Bergelson, argue in favour of property rights in personal data that address the shortcomings of tort law in the US legal system.[788] Torts do not have a preventative function; they provide remedies for committed wrongs.[789] Property rights will provide individuals with default entitlements that allow them to control the dissemination of their personal information.[790] On the other hand, tort law operates on a liability principle that allows the use of personal data without consent, as long as the affected individual is adequately compensated for any harm caused by such usage.[791] However, it is argued that this would not be efficient as the determination of damages requires resources such as the courts.[792] In contrast, property rights do not require the use of state resources because the individual with whom the data is associated is allocated default ownership, giving the individual the freedom to choose who to share their personal data with, for what purposes, and for how much.[793]

UNIVERSITY of the
WESTERN CAPE

A third economic argument advanced by US scholars in favour of propertisation is based on the development of a data protection system that is dependent on the interplay of legislative rules, technology and market tools to secure a proper level of information privacy.[794] Lessig, a proponent of this approach, states that data is an asset that has commercial value.[795] He suggests that each individual be assigned a property interest in their own personal data and employ

[786] Posner R 'The Economics of Privacy' (1981) 71 *The American Economic Review* 405 405. See also Cofone I (2017) 525–26. For example, an employer may not be able to implement effective health programmes for employees if privacy policies place restrictions on employers from gaining access to health information of employees.

[787] Posner R 'The Right to Privacy' (1977) 12 *Georgia Law Review* 393 398 argues that individuals should not own their personal information as they would withhold it from the market leading to inefficiencies. Kang J (1998) 1246–53 contends that individuals should own their personal information as they would incur substantial costs to determine what information has been collected and how it is being used if the initial entitlement is given to a data collector. See also Purtova N (2009) 514.

[788] Bergelson V (2003) 383.

[789] See 3.3.1 and 4.5 above.

[790] Cofone I (2017) 543.

[791] Calabresi G & Melamed D 'Property Rules, Liability Rules, and Inalienability: One View of the Cathedral' (1972) 85 *Harvard Law Review* 1089 1092–93.

[792] Purtova N (2009) 516–17.

[793] Bergelson V (2003) 428.

[794] Cohen J 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 *Stanford Law Review* 1373 1437; Purtova N (2009) 517.

[795] Lessig L *The Architecture of Privacy* (1998) 63.

https://uwcscholar.uwc.ac.za/home

Privacy Enhancing Technologies (PETs) to exercise control over their personal data.[796] PETs allow information to be encrypted, as is the case with copyright.[797] Recognising property rights in personal data would compel businesses to negotiate with individuals regarding the use of their data and encourage the development of PETs to better protect the privacy of the individual.[798] Negotiation will lead to the creation of a free market in personal data where individuals and businesses will agree on a price to be paid for the use of such data.[799] While such an approach also provides an economic argument for recognising property rights, it is based more on data protection considerations than market efficiencies.

4.9.3 Significance of ownership

As a starting point, it is notable that the US does not legally recognise property rights in personal data.[800] This is so despite personal data being treated as a commodity and the individual being identified as a trader in such a commodity.[801] Moreover, personal data as a commodity suggests that it is something that can be controlled and is therefore susceptible of ownership. In other words, personal data is a commodity that may be the object of a property entitlement. Property rights are based on the idea that there is an inherent connection between the individual and his personal data.[802] Some scholars conceptualise control as being directly linked to the idea of ownership, which suggests being entitled to trade and exchange personal data in the marketplace.[803]

The property rules outlined above consider property rights in personal data primarily from an economic or utilitarian perspective. In other words, the purpose of vesting property rights is to ensure that the flow of information is not impeded. However, the main drawback of these arguments is that they only consider property rights in terms of absolute ownership. These rules

[796] Lessig L *Code Version 2.0* (2006) 228.
[797] Lessig L 'Privacy as Property' (2002) 69 *Social Research* 247 250.
[798] Lessig L (2006) 228; Purtova N (2009) 517; Trakman L, Walters R & Zeller B 'Is Privacy and Personal Data Set to Become the New Intellectual Property?' (2019) 50 *International Review of Intellectual Property and Competition Law* 937 948.
[799] Lessig L (1998) 63.
[800] Samuelson P 'Privacy as Intellectual Property?' (1999) 52 *Stanford Law Review* 1125 1131; Hazel S 'Personal Data as Property' (2020) 70 *Syracuse Law Review* 1055 1058.
[801] See 4.2 above.
[802] Bergelson V (2003) 430; Purtova N (2009) 508.
[803] Lazaro C & Le Métayer D 'The Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12 *SCRIPTed* 3, 8–9; Solove D 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) 53 *Stanford Law Review* 1393 1446.

https://uwcscholar.uwc.ac.za/home

essentially aim to determine whether default ownership should go to the individual associated with the data or the party wishing to use such data as a function of the market. As a result, a significant portion of the literature focuses on debates pertaining to the absolute ownership of personal data.[804] It is submitted that this constitutes a narrow view of the meaning of property.

From a South African perspective, it is significant to note that s 25 of the Constitution is concerned with the protection of property including, but not limited to, the protection of rights and interests in property. Section 25 does not refer to ownership. When its provisions are properly interpreted contextually, purposively, and through the prism of s 39(1) of the Constitution, it becomes clear that s 25 does not have a narrow aim, namely, the mere protection of ownership in property.[805] As such, the control in a property regime may be understood as a bundle of rights as opposed to a 'despotic dominion over a thing'.[806] The exercise of absolute dominion is rendered impossible due to the limitations imposed by the rights and interests of others on one's own rights and entitlements. These entitlements will be explored further in chapter five within the framework of the data protection instruments of the EU.[807]

4.10 CHARACTERISTICS OF PROPERTISED PERSONAL INFORMATION

UNIVERSITY of the WESTERN CAPE

The objections to property rights in personal data is that the purported propertisation thereof does not meet the criteria to qualify as property. Commodification essentially embodies the core features of property, namely exclusivity and transferability. The following subsections will explore the alienability and excludability attributes of property, and then these attributes will be re-evaluated in the context of personal information.

4.10.1 Alienability

Alienability or separability, insofar as it relates to personal information, is a contentious issue. Arguments against propertisation are predicated on the idea that if something is 'property', it ought to be completely alienable. Litman argues that a property model would encourage transactions in data that most individuals prefer to discourage, and that alienability, which is an

804

805 *National Credit Regulator v Opperman* 2013 (2) SA 1 (CC) para 61.

806 Schwartz P (2004) 2094.

807 See 5.4.1 below.

https://uwcscholar.uwc.ac.za/home

inherent feature of property, would empower the data collector rather than the data subject by vesting control over the personal data in the data collector.[808] Similarly, Cohen is critical of the idea of recognising property rights in personal data, as it would enable more trade in personal data and consequently result in less privacy.[809] Samuelson notes that alienability is a ubiquitous feature of property rights systems, in which a property buyer can freely transfer to a third party whatever interest he or she acquired from the initial seller. Consequently, an individual may not be able to control the further transfer of his or her personal data, thereby lessening the control that the individual initially had.[810] According to Litman, referring to something as 'property' implies that it is transferable.[811]

It is submitted that the argument that property demands full alienability ought to be rejected for several reasons. First, Purtova states that 'unlimited market alienability is a myth' since many goods that could constitute property are heavily regulated.[812] For example, some intellectual property rights, such as patents, trademarks and copyrights, are governed by statutory laws that allow for restricted rights to be granted to anyone seeking to utilise and profit from such property. Secondly, the concept of alienability is flexible enough to accommodate alternative interpretations. In this regard, Schwartz proposes a hybrid inalienability model or alienability with limitations model that combines property rights and regulation to address the commodification of personal information.[813] The hybrid inalienability model comprises five elements, namely:[814]

(i) limitations on the alienability of personal information - To mitigate market failures associated with the personal trade where the data subject consents to the use of his personal information but subsequently loses control with respect to further processing of such data, Schwartz proposes a property regime in terms of which 'the burden of a property right "runs with the asset"'. This imposes a use-transferability restriction on any subsequent processing of personal information that

[808] Litman J (2000) 1303.
[809] Cohen J (2000) 1391.
[810] Samuelson P (1999) 1128.
[811] Litman J (2000) 1296.
[812] Purtova N 'Property in personal data: Second life of an old idea in the age of cloud computing, chain informatisation, and ambient intelligence' in Gutwirth S et al (eds) *Computers, Privacy and Data Protection: an Element of Choice* (2011) 59.
[813] With this hybrid model, Schwartz aims to address the concerns raised in 4.6 about the propertisation of personal information.
[814] Schwartz P (2004) 2094–116.

https://uwcscholar.uwc.ac.za/home

binds third parties and therefore allows the data subject to retain an element of control over his personal information even in transactions where he is not a party;

(ii) default rules - In conjunction with a use-transferability restriction, a default rule that forces disclosure of the terms of trade must be implemented. In this regard, Schwartz suggests an opt-in default to reduce information asymmetry by compelling the data processor wishing to make use of the personal information to disclose how such information will be processed. Moreover, hybrid inalienability 'would permit the transfer for an initial category of use of personal information, but only if the customer is granted an opportunity to block further transfer to unaffiliated entities';

(iii) right of exit – This element provides for a data subject to withdraw from a transaction after having opted-in or consented to the processing of personal information and the right to re-enter data trades. It also includes the right to remove or disable tracking technologies;

(iv) damages – An enforcement scheme premised on liquidated damages, preferably through legislation, may serve as a deterrent against the abuse and the unlawful processing of personal information and encourage privacy and data protection compliance; and

(v) monitoring and oversight – Institutions are necessary to assist in ensuring compliance with processes that exist for the exchange of personal information and to detect privacy infringements. Such a model involves the decentralisation of the market-making and oversight functions.

In terms of Schwartz's model, the opt-in default rules permit an initial transfer of personal data from the individual, provided the individual is afforded the opportunity to stop further transfers or use by third parties.[815] Similar to this, copyright uses a hybrid inalienability model, allowing one person to exploit a work but prohibiting the transfer of those rights to another.[816] However, to prevent copyright from stifling the flow of knowledge, certain exceptions are permitted, such

[815] Schwartz P (2004) 2098.
[816] Cohen J (2000) 1429.

UNIVERSITY of the WESTERN CAPE
https://uwcscholar.uwc.ac.za/home

as allowing such works and materials to be used for private or research purposes.[817] For example, copyright protects many of the works and materials this dissertation references. If these exceptions did not exist, then writing this dissertation would not be possible. In light of the above, it is important to note that the claim that property rights must be fully alienable is a fallacy. Therefore, Samuelson's assertion that alienability is a ubiquitous feature of property rights must be qualified to the extent that partial alienability or inalienability, however it is considered, is sufficient.

The other significant aspect is that the rights granted are enforceable against the world. If one uses the Schwartz hybrid inalienability model, only the party permitted to use the personal information may do so. As the model precludes personal information from being transferred unless consent is obtained, no third party may use the personal information. The frameworks for data protection legislation, such as POPIA and the GDPR, are similarly based on this hybrid inalienability model, which will be discussed further in chapter five.[818]

UNIVERSITY of the
WESTERN CAPE

4.10.2 Excludability

Intangible goods are generally regarded as public goods.[819] Public goods are characterised by non-excludability and non-rivalrous consumption.[820] Some scholars argue that information is a public good.[821] It is agreed that information is non-rivalrous because a single piece of information can be used by many people at the same time without being used up.[822] The claim that personal information is non-excludable, on the other hand, must be rejected. Despite its intrinsic non-rivalrous properties, the excludability of information depends on 'various extrinsic factors' such as the legal position pertaining to such property.[823]

---

[817] See s 12 of the Copyright Act 98 of 1978, which sets out exceptions in which fair use of a protected work is permitted without the need to obtain permission from the copyright owner.
[818] See 5.4.1 below.
[819] Karjiker S 'Justifications for copyright: The economic justifications' (2014) 4 *South African Intellectual Property Law Journal* 13 25.
[820] Schwartz P (2004) 2085.
[821] Lipton J 'Information property rights: Rights and responsibilities' (2004) 56 *Florida Law Review* 135 140–41; Schwartz P (2004) 2084–85.
[822] Nimmer R & Krauthaus P (1992) 105. People can sell information to another but still retain the information and use it for their own purposes. Oil, in contrast, has a finite quantity since it is a physical good.
[823] Karjiker S (2014) 26.

https://uwcscholar.uwc.ac.za/home

According to Gray, a resource can only be propertised if it is excludable, that is, if it can be controlled or used to the exclusion of others.[824] Baron states that the notion of excludability is central to the concept of property because it provides a real right to exclude others from using a resource.[825] In this context, 'property' denotes the relationship between persons in relation to that resource or object.[826]

Significantly, intellectual property, such as copyright, is considered a public good in economic terms.[827] Advocating for property rights in personal information, therefore, faces similar challenges to copyright, given its intangible and non-excludable nature. However, copyright is recognised as property under both private law and constitutional law.[828] Gray states, with merit, that a resource is excludable if it is feasible for a person to exert regulatory control over others' access to the various benefits of that resource.[829] In this regard, government regulation plays an important role in the recognition and expansion of property rights, particularly in the case of intellectual property.[830] For instance, copyright protection entails granting the copyright holder certain rights to exclude others from using the resource. Similarly, in the context of data protection, it may be argued that FIPSs-based data protection instruments, such as POPIA in South Africa,[831] the GDPR in the EU,[832] and the CCPA in the state of California,[833] grant limited exclusionary interests in personal information that allow the holder of the default entitlement to exclude others from using that resource. Victor states, with merit, that these protections function like regulated property schemes and can be best understood in property terms.[834] This aspect will be delved into further in chapter five.

[824] Gray K 'Property in thin air' (1991) 50 *Cambridge Law Journal* 252 268.
[825] Baron J (2012) 386–87.
[826] Muller G et al *Silberberg and Schoeman's The Law of Property* 6 ed (2019) 1.
[827] Karjiker S (2014) 25.
[828] See also 6.4 below.
[829] Gray K (1991) 268.
[830] Karjiker S *Open-Source Software and the Rationale for Copyright Protection of Computer Programs* (unpublished LLD thesis, University of Stellenbosch, 2013) 14.
[831] See 3.3.3 above.
[832] See 5.3.3 below.
[833] See 4.7.4 above.
[834] Victor J (2013) 522. See also 5.4.1 below.

https://uwcscholar.uwc.ac.za/home

4.11 CONCLUSION

The purpose of this chapter was to present an overview of the US data protection system and to understand the underlying dynamics that shaped the approach to dealing with personal data. At the outset, it was established that there is a correlation between marketplace discourse and the role that the data protection system is expected to fulfil. The data protection system exists to primarily protect the individual as a market participant and to facilitate the exchange of personal data. In so doing, the interests of companies that require personal data to innovate are balanced against the privacy interests of the individual as a consumer of information goods and services. From an American perspective, the importance of personal data can be attributed to its being perceived as a commodity and an indispensable resource for innovation to foster economic growth. Consequently, the privacy rights of individuals are considered secondary to innovation interests and are deliberately framed around supporting and encouraging innovation and the free flow of information.

It was established that the data protection system was conceived as one of secrecy insofar as it relates to tort law and the constitutional right to privacy. Tort provides only negative rights and does not offer adequate safeguards to prevent the unlawful processing of personal data. Constitutional remedies are limited as they apply only to government activities. They have no horizontal application and therefore do not regulate the large volumes of personal data that are collected and processed by the private sector. Subsequently, sectoral laws, focusing on specific types of information, were introduced to provide individuals with positive rights, giving them greater control over the processing of their information and improving data protection. However, these sectoral laws aim to facilitate the free flow of information and consequently offer individuals limited privacy protection while imposing relatively weak obligations on companies wishing to process personal data. The limitations of the US data protection system therefore spawned the idea of property rights in personal data.

In the US, personal data is treated as a commodity. Consequently, the arguments advocating for property rights in personal data are predominantly based on economic grounds. Such rights would serve to facilitate the market exchange of personal data while simultaneously providing data protection. From an economic perspective, property rights aim to efficiently regulate the use of resources by empowering individuals to decide how their personal data ought to be used and by whom. Despite the apparent weaknesses in the US data protection law, it is argued that the entire legal structure is designed to follow market principles when handling personal data.

https://uwcscholar.uwc.ac.za/home

It may be further argued that this is purposefully done to maximise economic benefits. However, it is submitted that the US will not legally recognise property rights in personal data as this may stifle the free flow of data.

Given the widespread commodification of personal data, the question arises as to whether this will be handled any differently in rights-based jurisdictions, such as South Africa and the EU. The next chapter examines the propertisation debate in the EU against the backdrop of a human rights culture, as well as property traits like as alienability and excludability in the context of data protection rules.

UNIVERSITY of the
WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

CHAPTER FIVE: THE EUROPEAN DATA PROTECTION FRAMEWORK AND THE PERSONAL INFORMATION TRADE

5.1 INTRODUCTION 144

5.2 HUMAN RIGHTS DISCOURSE 145

5.3 REGULATION OF DATA PROTECTION IN THE EU 149

5.3.1 Charter of Fundamental Rights of the European Union 153

5.3.2 Directive 95/46/EC 156

5.3.3 General Data Protection Regulation 158

5.3.3.1 Selected principles 159

5.3.3.1.1 Lawfulness, fairness and transparency 159

5.3.3.1.2 Purpose limitation 161

5.3.3.1.3 Data minimisation 162

5.3.3.2 Lawful grounds for processing data 163

5.3.3.2.1 Consent 163

5.3.3.2.2 Contractual necessity 165

5.3.3.2.3 Legitimate interests 168

5.4 PROPERTY RIGHTS IN PERSONAL INFORMATION 169

5.4.1 GDPR: Property-like entitlements 170

5.4.1.1 Consent 171

5.4.1.2 The right to data portability 172

5.4.1.2.1 Control over data sharing 174

5.4.1.2.2 Control over (re-)uses of personal information 175

5.4.1.2.3 Data portability and property rights 175

5.4.1.3 The right to erasure (right to be forgotten) 176

5.4.1.3.1 Right to erasure and property rights 179

5.5 DIGITAL CONTENT DIRECTIVE 180

UNIVERSITY of the WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

5.5.1 Personal information as counter-performance 181
5.5.2 Convergence between personal information as counter-performance and the human rights foundations of data protection 182
5.6 CONCLUSION 186

UNIVERSITY of the
WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

5.1 INTRODUCTION

In chapter four, it was concluded that the US places considerable weight on marketplace discourse. Moreover, the US data protection regulatory framework encourages the treatment of personal data as a tradeable commodity. In the EU,[835] the purported commodification of personal data has not gone unnoticed. In 2012, the then Vice-President of the European Commission (EC), Viviane Reding, described personal data as 'valuable assets', the 'currency of today's digital market' and implied that data belonged to individuals.[836] Subsequently, in 2016, Margrethe Vestager, a commissioner of the EC, echoed similar sentiments by stating that 'personal data has become a valuable commodity'.[837] However, the European Data Protection Supervisor (EDPS) has, from a legal standpoint, rejected the idea that personal data is commodifiable or recognisable as a form of currency from an EU perspective.[838] This seems to suggest some political and legal differences concerning the treatment of personal data and underscores the obstacles confronting the EU.

In the EU, an individual's right to the protection of personal information is entrenched as a fundamental right.[839] Fundamental rights are characterised as being (1) universal and inalienable, (2) indivisible, (3) interdependent and (4) imprescriptible.[840] Since fundamental rights are conceived as closely linked to individuals by reason of their personhood and are necessary for maintaining a person's dignity, they are treated as non-commodifiable rights in the EU.[841] Therefore, the stance of the EU is that personal data cannot be bought or sold. Given the constitutional right to privacy in South Africa and the relevance of data processing in

---

[835] The EU currently comprises of 27 countries, namely Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.

[836] Reding V 'The EU data protection reform 2012: Making Europe the standard setter for modern data protection rules in the digital age' (2012) available at *http://europa.eu/rapid/ press-release_SPEECH-12-26_en.htm* (accessed 4 May 2024).

[837] Vestager M 'Making Data Work for Us' (2016) available at *http://web.archive.org/web/ 20161015230600/http:/ec.europa.eu/commission/2014-2019/vestager/announcements/making-data-work-us_en* (accessed 4 May 2024).

[838] EDPS *Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content* (2017) paras 15–17.

[839] See 5.2 below.

[840] Custers B & Malgieri G 'Priceless data: Why the EU fundamental right to data protection is at odds with trade in personal data' (2022) 45 *Computer Law & Security Review* 1 6. Universal means that everyone is entitled to such rights by virtue of being human. A right is inalienable if it cannot, voluntarily or otherwise, be taken away. Indivisibility means that all rights are equal and do not follow a hierarchical order. Fundamental rights are interdependent, so exercising one right will affect another. Rights are imprescriptible, which means that they will not expire over time.

[841] Prins C 'Property and privacy: European perspectives and the commodification of our identity' in Guibault L & Hugenholtz P (eds) *The Future of the Public Domain* (2006) 234.

https://uwcscholar.uwc.ac.za/home

fostering values such as dignity and autonomy, it is reasonable to submit that a comparable legal landscape exists in South Africa.[842] However, this position calls for reappraisal given that the personal information trade is a universal phenomenon.

In contrast to the US, the EU possesses a well-established data protection system that affords individuals control over their personal information to prevent misuse or wrongful disclosures. Moreover, in light of the notion that fundamental rights are non-commodifiable, establishing property rights in personal information would be contrary to the EU's fundamental rights-based approach. Despite this approach, the chapter argues that the EU data protection regime contains property-like features, such as alienability and excludability, as identified in the previous chapter.

While data protection is recognised as a fundamental right, it is acknowledged that personal information is also considered an important commodity and a valuable asset.[843] The tension between the two conflicting regulatory areas epitomises the challenge facing the EU. This chapter begins by providing an overview of the history and legal justification that shaped the EU's data protection framework. As the EU places significantly more emphasis on the fundamental rights of data subjects than the US, the chapter explores selected aspects of the EU's rights-centred data protection framework. The EU legal framework will be discussed as it pertains to the processing of personal information from a fundamental rights perspective and the growing significance of data as a central feature of commercial exchanges. In view of the growing importance of personal information in an economic context, the question arises whether the treatment of personal information as something that is considered non-commodifiable is still relevant given current data practices.

5.2 HUMAN RIGHTS DISCOURSE

A rights-based framework focuses on the individual whose data is processed 'anchored in interests of dignity, personality, and self-determination', a consequence of the experiences with fascism and Nazism during World War II.[844] Intrusions into the privacy of individuals were

[842] See 3.5 above.

[843] Lynskey O (2015) 2; Bottis M & Bouchagiar G 'Personal data v. Big data: Challenges of commodification of personal data' (2018) 8 *Open Journal of Philosophy* 206 206; Purtova N 'Property in personal data: A European perspective on instrumentalist theory of propertization' (2010) 2 *European Journal of Legal Studies* 193 200.

[844] Schwartz P & Peifer K 'Transatlantic data privacy law' (2017) 106 *Georgetown Law Journal* 115 123. This may be contrasted with the 'privacy consumer' in the US context. For more information see 4.2 and 4.7 above.

https://uwcscholar.uwc.ac.za/home

commonplace as a result of clandestine and large-scale operations carried out under the guise of national security or to identify members of undesirable groups.[845] Consequently, the recognition and safeguarding of dignity and self-development are central to the development of data protection rights from an EU perspective. As is the case with South Africa, dignity serves to inform the content and limits of fundamental rights, such as the right to data protection.[846] This can be attributed to both the EU and South Africa having experienced distressing historical periods in which individuals were denied dignity and respect.[847]

Given that data protection is a fundamental right, the EU rights-based framework does not conceive of personal data as an economic asset.[848] The EDPS has endorsed this position, asserting that personal data cannot be considered a commodity.[849] Therefore, the notion of personal data commodification does not fit within the EU rights-based data protection regime. However, the EU recognises that data is a necessary resource to foster and promote economic growth, job creation and enhanced societal progress.[850] Data supports economic development and is the basis for innovative products and services, increased productivity and resource efficiency across all sectors of the economy, including government.[851] Data-driven innovation promises enormous benefits for citizens, including better energy consumption, product, material, and food traceability, improved well-being and better health care.[852] It is expected that the estimated impact of the data economy on the GDP of the EU will steadily increase over the next few years.[853]

To maximise the growth potential of the data economy, the European Commission (EC) has prioritised the creation of a Digital Single Market (DSM), which will facilitate the free movement of goods, persons, services, and capital and where individuals and businesses,

---

[845] Schwartz P & Peifer K (2017) 123.

[846] Lynskey O (2015) 94–101. Lynskey highlights that while the right to data protection is based on dignity, the exact content of 'dignity' as a concept needs to be clarified.

[847] See also 3.6 above.

[848] EDPS (2017) para 16.

[849] EDPS (2017) para 14. Rouvroy A & Poullet Y 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Gutwirth S et al (eds) *Reinventing Data Protection?* (2009) 50 argue that commodification of personal data would lead to individuals waiving their rights to data protection. I do not agree with Rouvroy and Poullet's argument as it is possible to distinguish between the right to data protection and the actual personal data.

[850] EC *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Building a European Data Economy* (2017) 2.

[851] EC *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data* (2020) 2.

[852] EC *A European Strategy for Data* (2020) 2.

[853] See 1.2 above.

https://uwcscholar.uwc.ac.za/home

irrespective of nationality or place of residence, can transact online under conditions of fair competition with high levels of consumer and data protection.[854] The strategy of the DSM is built on three policy pillars, namely (1) better access for consumers and businesses to online goods and services across Europe, (2) ensuring optimum conditions for digital networks and services to flourish and (3) maximising the growth potential of the digital economy.[855] The DSM will harmonise e-commerce rules across the EU relating to online and digital cross-border purchases as well as minimise barriers to cross-border trade, including data flows and data ownership.[856]

Like the US, the EU recognises that the free flow of information is an essential element for innovation and a well-functioning data economy.[857] In contrast to the US, the EU actively advocates that the free flow of information ought to be respectful of human rights.[858] This approach stems from the fundamental tension between asserting dignity as a value that underpins data protection and the desire to encourage the data trade. Consequently, the EU is constantly confronted with the task of striking a harmonious equilibrium between safeguarding data and facilitating the unrestricted movement of data.[859] According to Reding, a uniform and comprehensive data protection framework will reinforce individuals' fundamental right to data protection and unlock the potential of the DSM by fostering economic growth, innovation, and job creation.[860] These dual economic and rights-based objectives underpin EU data protection law.[861] The EC duly acknowledges: 'In the digital era, promoting high standards of data protection and facilitating international trade must… necessarily go hand in hand.'[862] In this regard, South Africa faces a similar challenge with the adoption of its own data protection legislation.[863]

[854] EC *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe* (2015) 3.
[855] EC *A Digital Single Market Strategy for Europe* (2015) 3.
[856] EC *A Digital Single Market Strategy for Europe* (2015) 4–14.
[857] EC *Building a European Data Economy* (2017) 5–8.
[858] EC *A European Strategy for Data* (2020) 4–5.
[859] This will be discussed further in 5.3 below in the context of statutory protection.
[860] Reding V (2012) 128.
[861] Lynskey O (2015) 8.
[862] EC *Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World* (2017) 6.
[863] See 3.3.3 above.

https://uwcscholar.uwc.ac.za/home

Implementing data protection to regulate data flow has its roots in the right to privacy and serves to foster other fundamental freedoms, such as autonomy and human dignity.[864] In the EU, data protection, though initially driven by economic reasons, is now firmly rooted within a human rights framework.[865] This approach is predicated on the view that by strengthening individuals' trust and confidence in the digital environment and enhancing legal certainty, it will result in a regulatory environment that is conducive to the development of innovative goods and services necessary to exploit the potential of the data-driven economy.[866] Fostering trust in innovation is also a key objective for the US government, as it stimulates economic expansion.[867] Therefore, it would be entirely reasonable to claim that the EU has similar aspirations to the US insofar as it relates to exploiting personal data but doing so under the guise of dignity. The questions then arise as to whether the intention to position data processing within a rights-based framework has any bearing on the actual treatment of personal data and the personal data itself. Put simply, it must be enquired if the use of dignity-based processing in pursuit of innovation makes personal data less of a commodity.

The next section commences with an overview of the various regulatory initiatives that aim to enhance personal information protection and regulate the movement of personal information, which is central to promoting the objectives of the DSM. This overview considers only a limited number of supranational instruments most relevant to the study and does not include domestic laws of EU member states that should be adopted or amended to implement the standards outlined in the supranational instruments.[868] The discussion will therefore focus on the European perspective at the EU level.[869] As the EU consists of several individual member

---

[864] Abdulrauf L & Fombad C 'Personal data protection in Nigeria: Reflections on opportunities, options and challenges to legal reforms' (2017) 38 *Liverpool Law Review* 105 112–16.

[865] Tzanou M *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (2017) 14–8; Van der Sloot B 'Legal fundamentalism: Is data protection really a fundamental right?' in Leenes R et al (eds) *Data Protection and Privacy: (In)visibilities and Infrastructures* vol 36 (2017) 6–8.

[866] Reding V (2012) 124; EC *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards a Thriving Data-Driven Economy* (2014) 11; EC *A Digital Single Market Strategy for Europe* (2015) 13; EC *Building a European Data Economy* (2017) 3.

[867] See 4.2 above.

[868] The relevant part of art 288 of the Consolidated Version of the Treaty on the Functioning of the European Union 2012 (OJ C 326/47) (TFEU) reads: 'To exercise the Union's competences, the institutions shall adopt regulations, directives… A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods.'

[869] For an overview of the functions of the various EU institutions, see EC *How the European Union Works: Your Guide to the EU Institutions* (2014) 5 available at https://data.europa.eu/doi/10.2775/11255 (accessed 10 February 2022).

https://uwcscholar.uwc.ac.za/home

states, it ought to be representative of those states' shared or common interests, such as the DSM, data protection, and respect for human rights.

5.3 REGULATION OF DATA PROTECTION IN THE EU

Privacy and data protection are intertwined.[870] The emergence and application of data protection were driven primarily by privacy concerns brought about by new technologies.[871] However, Gutwirth and De Hert explain, correctly in my view, that data protection and privacy protection are complementary tools directed towards achieving similar objectives, namely, control and limitation of power.[872] As such, data protection should not be equated with privacy, as data protection may protect the interests of privacy as well as values that are not at the core of privacy and therefore, conceptually, can be viewed in either broad or more limited terms regardless of its relationship with privacy.[873] This intersection between privacy and data protection was discussed in chapter three.[874]

The right to privacy is a fundamental right enshrined in various human rights instruments, such as the Universal Declaration of Human Rights (UDHR)[875] and the European Convention on Human Rights (ECHR),[876] which guarantees the right to respect for, among other things, private and family life and establishes the conditions under which restrictions of this right are permitted. In the context of privacy and family life, the right to privacy has been interpreted to include the right to data protection, even though data protection is not explicitly mentioned in

[870] Andrade N 'Data protection, privacy and identity: Distinguishing concepts and articulating rights' in Fischer-Hűbner S et al (eds) *Privacy and Identity Management for Life* 352 (2010) 91.

[871] Van der Sloot B in *Data Protection and Privacy: (In)visibilities and Infrastructures* (2017) 5; Andrade N in *Privacy and Identity Management for Life* (2010) 91.

[872] Gutwirth S & De Hert P 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in Claes E, Duff A & Gutwirth S (eds) *Privacy and the criminal law* (2006) 66–7.

[873] Andrade N in *Privacy and Indentity Management for Life* (2010) 94–8. See 3.5 above.

[874] See 3.4 above.

[875] Article 12, Universal Declaration of Human Rights 1948. The UDHR was adopted by the General Assembly of the United Nations, resolution 217 (III) of 10 December 1948. UN Doc. A/3/810 (1949).

[876] Article 8, European Convention on Human Rights 1950. The ECHR was adopted by the Council of Europe on 4 November 1950 in Rome, and entered into force on 3 September 1953. The ECHR serves as an international treaty and binds the contracting states as part of its body of international law.

https://uwcscholar.uwc.ac.za/home

the aforesaid instruments.[877] In this regard, South Africa has taken a similar approach, interpreting the right to data protection as stemming from the right to privacy.[878]

Pearce explains that despite the importance of art 8 of the ECHR in affirming the importance of the right to private and family life, it has significant shortcomings concerning data protection.[879] These limitations encompass the absence of direct applicability to the private sector, its scope being restricted to only personal information regarded as private, and the absence of a right that provides access to personal information.[880] Unlike the almost exclusively negative constitutional rights of the US,[881] which bind only the government and have no application with respect to private relationships, the ECHR may impose positive obligations on contracting states to take measures that are applicable between private parties.[882] Nevertheless, the EU encounters additional complexity since various member nations may possess divergent interpretations regarding an identical matter, which may explain the need for supranational legal instruments. By way of comparison, constitutional rights in South Africa are binding on all organs of state and all persons, natural and juristic.[883] The horizontal effect places individuals at the core of the data protection framework, recognising them as a bearer of rights.[884]

The difference between private and personal information was explored in chapter three.[885] It is submitted that while there exists an overlap between the two concepts, data protection is concerned with personal not private information. Given contemporary data practices and novel

[877] Purtova N 'Property in personal data: A European perspective on instrumentalist theory of propertization' (2010) 203–4; González Fuster G & Gellert R 'The fundamental right of data protection in the European Union: In search of an uncharted right' (2012) 26 *International Review of Law, Computers & Technology* 73 74; *Joined Cases C-293/12 and C-594/12 Digital Rights Ireland v Minister for Communications, Marine and Natural Resources, Seitlinger and Others* (2014) ECLI:EU:C:2014:238 para 48; Yakovleva S 'Should fundamental rights to privacy and data protection be a part of the EU's international trade "Deals"?' (2018) 17 *World Trade Review* 477 485.

[878] See 3.4 above.

[879] Pearce H 'Personality, property and other provocations: Exploring the conceptual muddle of data protection rights under EU Law' (2018) 4 *European Data Protection Law Review* 190 195. Pearce mentions specifically that art 8 was not flexible enough to sufficiently protect individuals from the harms stemming from the misuse of personal information linked to the growing use of information technology.

[880] Purtova N 'Private law solutions in European Data protection: Relationship to privacy, and waiver of data protection rights' (2010) 28 *Netherlands Quarterly of Human Rights* 179 185.

[881] See 4.6 above.

[882] European Court of Human Rights *Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life, Home and Correspondence* (2023) 175.

[883] See 3.6.2 above.

[884] Schwartz P & Peifer K (2017) 126.

[885] See 3.3.1 above.

https://uwcscholar.uwc.ac.za/home

business models that rely on the exchange of personal data, the privacy expectations of what is now considered reasonable may not fit the notion of 'private', according to the ECHR.[886]

The determination of what constitutes private information depends on whether a reasonable expectation of privacy exists. As was discussed in chapter three, private information does not necessarily equate to personal information.[887]

As is the case with the US and South African constitutions, the ECHR does not contain provisions that provide individuals with active control over their personal data. Some scholars view this as shortcomings or limitations.[888] I differ slightly from the scholars, as I argue that it is not the purpose of a document like a constitution to provide such rights. It is submitted that a shortcoming will be apparent in those instances where the principle of subsidiarity lacks constitutional support.

Although art 8 has evolved to be more responsive to technological advancements by introducing more elements of positive obligations, it offers only limited data protection. Moreover, Mostert et al conclude that the right to data protection includes certain core elements that are not relevant for privacy, and therefore the right to privacy does not guarantee a similar level of protection as that offered by the right to data protection.[889] The rise of the data processing industry in Europe during the 1970s led to the enactment of the first data protection laws.[890] Tzanou notes that the EU initially conceived data protection in market terms with the goal of fostering economic interests by facilitating free and unimpeded transfers of personal information.[891] The OECD made an early attempt to ensure that the national laws of the various member states did not impede cross-border data flows.[892] The growth of the global economy increased the exchange and flow of personal information across national borders, necessitating the harmonisation of data protection laws to balance privacy protection for individuals while

[886] For example, the term 'private' is generally associated with the personal sphere, seclusion and concealing information.

[887] See 3.4 above.

[888] Purtova N 'Private Law Solutions in European Data Protection' (2010) 185; Naude A & Papadopoulos S 'Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments (1)' (2016) 79 *Journal of Contemporary Roman-Dutch Law* 51 56.

[889] Mostert M et al 'From privacy to data protection in the EU: Implications for big data health research' (2018) 25 *European Journal of Health Law* 43 50–1. These elements include data security measures, data quality requirements, and supervision by an independent authority. See also 3.4 above.

[890] Andrade N in *Privacy and Indentity Management for Life* (2010) 91; Lynskey O (2015) 3.

[891] Tzanou M (2017) 16.

[892] OECD *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980) 1–21.

https://uwcscholar.uwc.ac.za/home

enabling the free flow of information.[893] Tzanou states, with merit, that '[d]ata protection was not only born out of internal market concerns; its concept was also recognised as a dimension of privacy and its protection was dependent on it'.[894] The various data protection instruments enacted over the years reflect these dual objectives, as we will discuss below.

The introduction of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal information,[895] colloquially known as Convention 108, was precipitated by the limitations of art 8 of the ECHR and was adopted to safeguard fundamental rights such as the right to privacy and to ensure the free flow of information.[896] According to Convention 108, the purpose is to ensure that every individual, regardless of nationality or residence, has respect for his rights and fundamental freedoms, particularly his right to privacy, in the territory of each contracting country with regard to the automatic processing of personal data relating to him.[897] An analysis of Convention 108 is beyond the scope of this dissertation; however, it is notable for incorporating FIPs and promoting fundamental rights and freedoms, in particular the right to privacy, in relation to the automatic processing of personal information.[898] Despite not being recognised as a fundamental right in Convention 108,[899] data protection has evolved from being viewed purely as an economic concern to becoming increasingly closely tied with fundamental rights.[900]

The subsequent recognition of data protection as a new fundamental right alongside the right to privacy in the EU reflects 'fundamental social values in the era of rapid advancement of new technologies' and gives rise to identifiable rights and obligations.[901] Data protection as a fundamental right is underpinned by the interests of a person's dignity, personality and self-determination.[902] Rouvroy and Pollet are, however, critical of the right to data protection being

[893] Roos A 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124 *SALJ* 400 403–4.
[894] Tzanou M (2017) 17.
[895] Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981. Convention 108 was signed in 1981, and came into force in 1985 after ratification by the required number of countries.
[896] Yakovleva S (2018) 485.
[897] Article 1, Convention 108.
[898] Pearce H (2018) 195.
[899] Tzanou M (2017) 20.
[900] Taylor M 'The EU's human rights obligations in relation to its data protection laws with extraterritorial effect' (2015) 5 *International Data Privacy Law* 246 247. See also Tzanou M (2017) 17.
[901] Tzanou M (2017) 20. See also 3.5 above for a discussion on the distinction between the right to data protection and the right to privacy.
[902] Schwartz P & Peifer K (2017) 123.

https://uwcscholar.uwc.ac.za/home

placed on the same level as privacy and state 'it risks obscuring the essential relation existing between privacy and data protection and further estrange data protection from the fundamental values of human dignity and individual autonomy, foundational to the concept of privacy and in which data protection regimes have their roots…'.[903] Rouvroy and Pollet's viewpoint is rejected, as data protection offers individuals enhanced control over their personal information and, in so doing, reinforces the individual's rights to human dignity and autonomy.[904] Abdulrauf and Fombad contend, with merit, that despite data protection being of relatively recent origin, it does not fall below other fundamental rights.[905]

Entrenching data protection as a fundamental right means that it has 'vertical' application concerning government-on-private matters and 'horizontal' effects that reach within private-on-private relations.[906] The recognition of the horizontal direct effect of this right is particularly important given that it is often private entities that process personal information.[907] Brkan argues, correctly in my view, that permitting only a vertical direct effect of the right to data protection would prejudice data subjects as they would only be able to rely on such a right where the dispute involves a public authority processing the data.[908] Recognising data protection as a fundamental right imposes a constitutional obligation to enact statutory laws that regulate data use.[909] The sections that follow discuss selected legal instruments that are part of the EU data protection system.

5.3.1 Charter of Fundamental Rights of the European Union

Fundamental rights have long been recognised in treaties and applied by the courts as general principles of EU law.[910] However, a growing concern for fundamental rights and efforts to

[903] Rouvroy A & Poullet Y 'The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy' in Gutwirth S et al (eds) *Reinventing Data Protection?* (2009) 71–4.

[904] See 3.2.2 above.

[905] Abdulrauf L & Fombad C (2017) 116.

[906] Schwartz P & Peifer K (2017) 126.

[907] Brkan M 'The unstoppable expansion of the EU fundamental right to data protection: Little shop of horrors?' (2016) 23 *Maastricht Journal of European and Comparative law* 812 822; EDPS *Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content* (2017) para 63 states that the GDPR is intended to have horizontal application.

[908] Brkan M (2016) 823. See also the discussion on horizontality in 3.6.2 above. An inherent weakness of the US Constitution insofar as it applies to data protection is its lack of horizontal application. See 4.6 above.

[909] Schwartz P & Peifer K (2017) 127; Abdulrauf L & Fombad C (2017) 116.

[910] Douglas-Scott S 'The European Union and human rights after the Treaty of Lisbon' (2011) 11 *Human Rights Law Review* 645 648.

https://uwcscholar.uwc.ac.za/home

make them more visible to EU citizens culminated in the Charter of Fundamental Rights of the European Union (EUCFR)[911] being promulgated in 2000.[912] According to Douglas-Scott, the EUCFR is now the departure point text for the Court of Justice of the European Union (CJEU) assessment of fundamental rights within the EU.[913] The EUCFR was initially envisaged as a non-binding political document.[914]

The signing of the Treaty of Lisbon (Lisbon Treaty)[915] by EU member states in 2009 resulted in the EUCFR becoming binding constitutional law.[916] Article 6(1) of the Lisbon Treaty provides that '[t]he Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties'. Consequently, the EUCFR binds member states when implementing EU law, and it obliges EU institutions and bodies to respect the rights listed therein when fulfilling their treaty obligations. The EUCFR sets out, rather innovatively in a single document, a range of economic, social, civil and political rights drawn from various legislative instruments and, additionally, introduces new fundamental rights, such as the right to data protection, which previously did not exist.[917]

UNIVERSITY of the WESTERN CAPE

The EUCFR is unique in the sense that it protects both the right to privacy and the right to the protection of personal information in arts 7 and 8 respectively, as two distinct but overlapping fundamental rights.[918] Article 7 of the EUCFR provides that '[e]veryone has the right to respect for his or her private and family life, home and communications', while art 8 of the EUCFR reads as follows:

---

911 Charter of Fundamental Rights of the European Union (2000) OJ C364/01 and (2010) OJ C83/389.

912 European Union Agency for Fundamental Rights et al *Handbook on European Data Protection Law* (2018) 27–8; Tzanou M (2017) 19.

913 Douglas-Scott S (2011) 656. The EUCFR serves as the key constitutional document of the EU.

914 Douglas-Scott S (2011) 648; European Union Agency for Fundamental Rights et al (2018) 28.

915 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community 2007/C 306/01 2007. Signed on 13 December 2007 and entered into force on 1 December 2009.

916 Schwartz P & Peifer K (2017) 125; Tzanou M (2017) 17; European Union Agency for Fundamental Rights et al (2018) 28.

917 Douglas-Scott S (2011) 651. The preamble to the EUCFR reaffirms the fundamental rights as they result from 'the constitutional traditions and international obligations common to' EU member states, treaties, conventions, charters and case law. Data protection rules were already codified in certain instruments prior to its recognition as a fundamental right, such as, Convention 108 and Directive 95/46/EC, which is discussed in 5.3.2 below.

918 Hildebrandt M *Law for Computer Scientists and Other Folk* (2020) 128; Pearce H (2018) 196; Abdulrauf L & Fombad C (2017) 110–11; Lynskey O 'Deconstructing data protection in the EU legal order' (2014) 63 *International and Comparative Law Quarterly* 569 589–97.

https://uwcscholar.uwc.ac.za/home

'1. Everyone has the right to the protection of personal information concerning him or her.

2. Such 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.

3. Compliance with these rules shall be subject to control by an independent authority.'

Article 7 of the EUCFR embodies the rights guaranteed by art 8 of the ECHR,[919] while the introduction of art 8 of the EUCFR enshrines a new, distinct right to personal information protection.[920] Article 8 of the EUCFR incorporates some FIPs relating to (1) fair processing, (2) purpose specification, (3) lawful processing requiring consent or some other legitimate basis, (iv) rights of access and rectification and (4) a requirement for introduction for independent regulatory authorities to ensure compliance with data principles.[921] Data protection rights are not absolute and are subject to the general limitations clause.[922]

The EUCFR, in conjunction with the ECHR, serves as the foundational framework for fundamental rights in Europe. The CJEU has recognised the overlap of fundamental rights relating to privacy and data protection between the ECHR and the EUCFR.[923] In *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen (Schecke)*,[924] the CJEU combined the relevant sections from the EUCFR and ECHR, thereby formally enshrining data protection within the EU.[925]

[919] See art 52(3), EUCFR.

[920] González Fuster G & Gutwirth S 'Opening up personal data protection: A conceptual controversy' (2013) 29 *Computer Law & Security Review* 531 535. It is, however, acknowledged that certain elements contained in art 8 of the EUCFR are based on Directive 95/46/EC.

[921] Schwartz P & Peifer K (2017) 128.

[922] Douglas-Scott S (2011) 652. Article 52(1) of the EUCFR states that restrictions may be imposed on rights and freedoms provided such restrictions are aligned with the objectives of the EU and are not disproportionate and unreasonable.

[923] Schwartz P & Peifer K (2017) 125.

[924] Joined Cases C 92/09 and C 93/09 ECLI:EU:C:2010:662.

[925] Joined Cases C 92/09 and C 93/09 ECLI:EU:C:2010:662 para 52.

https://uwcscholar.uwc.ac.za/home

5.3.2 Directive 95/46/EC

The GDPR repealed Directive 95/46/EC (Data Protection Directive), [926] which played a crucial role in the EU data protection framework from 1995 until May 2018. Despite being no longer in effect, the Data Protection Directive is worth mentioning due to its historical contribution. The Data Protection Directive is rooted in human rights, which is evident in several recitals in the preamble.[927] Moreover, art 1 of the Data Protection Directive describes its purpose and object as protecting fundamental rights and freedoms, in particular the right to privacy with respect to the processing of personal information. Reding points out, with merit, that the Data Protection Directive enshrines 'two of the oldest and equally important ambitions…' in EU data protection, namely the right to data protection and the free flow of personal information.[928] This can be attributed to technology advancements that have not only created new possibilities but also presented privacy concerns.[929] In the EU's pursuit of establishing an internal market for data that is respectful of the dignity of individuals, there is an ongoing challenge to reconcile the conflicting interests. There appears to be a conscious effort on the part of the EU to play down the economic interests in data. This balancing act is evident in the rules governing the lawful processing of data, as will be discussed in the context of the General Data Protection Regulation (GDPR).[930]

UNIVERSITY of the
WESTERN CAPE

Lynskey observes that when the Data Protection Directive was enacted in 1995, only one percent of the EU population used the Internet at the time.[931] The adoption of the Data Protection Directive represented an attempt to harmonise data protection laws across EU member states.[932] Achieving harmonisation would prohibit member states from inhibiting the free movement of personal information between them on grounds related to the protection of the rights of individuals.[933] In other words, the intention was to encourage rather than prevent the free flow of information.

---

[926] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data 1995 Official Journal L 281/31.

[927] See recitals 1, 2, 3, 10, 33, 34 and 37 of the Data Protection Directive.

[928] Reding V (2012) 120.

[929] See 2.1 above.

[930] See 5.3.3 below.

[931] Lynskey O (2015) v.

[932] European Union Agency for Fundamental Rights et al (2018) 28–9; Lynskey O (2015) 8.

[933] Roos A (2007) 407.

https://uwcscholar.uwc.ac.za/home

The Data Protection Directive incorporated all the principles contained in Convention 108 and supplemented them with additional rules and provisions.[934] The Data Protection Directive, accordingly, regulated the processing of personal information of subjects by or on behalf of a data controller,[935] and established principles with which processing of all personal information were to comply.[936] The Data Protection Directive also provided for the establishment of independent supervisory authorities in each member state to monitor compliance with their national data protection laws.[937]

Despite the introduction of the Data Protection Directive as a detailed, comprehensive, and all-encompassing data protection framework, the inherent shortcomings of a directive meant that such provisions did not find direct application and had to be transposed into member states' national laws, resulting in diverse data protection rules and differing interpretations of the rules.[938] Reding claims, rightly so, that such divergence resulted in a fragmented legal framework, creating legal uncertainty and unequal protection for data subjects, increasing administrative costs for data controllers operating across borders, and adversely affecting the competitiveness of the EU.[939] Moreover, Pearce states that the efficacy of the Data Protection Directive was further challenged by technological advancements and the emergence of novel data mining and analytical technologies characteristic of the big data era.[940] Despite the fact that suitable rules existed, they could not be properly enforced due to their inherent limitations.

To remedy the shortcomings of the Data Protection Directive, the implementation of a regulation, as opposed to a directive, that has direct applicability in all member states was considered a means to provide enhanced legal certainty, improve protection for individuals and ensure a free flow of personal information.[941] Schwartz and Peifer state that the decision to replace the directive with a regulation highlights the importance of EU data protection as a statutory matter.[942] A regulation that has direct application in member states therefore precludes 'the cumulative and simultaneous application of different national data protection

---

[934] Pearce H (2018) 195; European Union Agency for Fundamental Rights et al (2018) 29.
[935] The South African equivalent of a data controller is the responsible party. See 1.5.4.3 above.
[936] Roos A 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position' (2007) 124 *SALJ* 400 407.
[937] Article 28, Data Protection Directive.
[938] European Union Agency for Fundamental Rights et al (2018) 29–30.
[939] Reding V (2012) 121.
[940] Pearce H (2018) 195.
[941] Reding V (2012) 121.
[942] Schwartz P & Peifer K (2017) 128.

https://uwcscholar.uwc.ac.za/home

laws'.[943] Therefore, realising the dual objectives of an adequate level of data protection and data flow can only be achieved through a harmonised regulatory system that is binding across the EU.

5.3.3 General Data Protection Regulation

The GDPR came into force on 25 May 2018 and replaced the Data Protection Directive. The GDPR was designed to address the shortcomings of the Data Protection Directive and respond to the challenges occasioned by the emergence of data mining and analytical technologies associated with big data.[944] While the Data Protection Directive aims to safeguard privacy, the GDPR focuses on data protection.[945] As such, the GDPR unanimously affirms the protection of fundamental rights, in particular the right to data protection.[946] Consequently, most references to 'privacy' have largely disappeared from the text and recitals of the GDPR.[947] In contrast, the purpose of POPIA is to give effect to the constitutional right of privacy.[948] It is submitted that this could be because, first, the Data Protection Directive was the blueprint for POPIA,[949] and secondly, at the time when the Constitution was drafted, the issue of data protection was generally unknown.

It is envisaged that the GDPR will play a central role in supporting the DSM. Establishing a more coherent data protection framework will promote trust and enhance legal certainty, which will foster the development of the digital EU economy.[950] The GDPR aims to ensure the free flow of personal information within the EU to allow for the proper functioning of the DSM.[951] The following subsections will review selected GDPR principles and grounds for processing personal information that are relevant in the context of business models based on large-scale

[943] Reding V (2012) 121.
[944] Pearce H (2018) 195; European Union Agency for Fundamental Rights et al (2018) 30.
[945] Lynskey O (2015) 10. Recital 1 of the GDPR states that data protection is a fundamental right and refers, among other things, to art 8 of the EUCFR as authority for adopting such a position.
[946] Mostert M et al (2018) 44. Article 1(2) of the GDPR states: 'This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.'
[947] Mostert M et al (2018) 46.
[948] See 3.3.3 above.
[949] Roos A 'The European Union's General Data Protection Regulation (GDPR) and Its Implications for South African Data Privacy Law: An Evaluation of Selected "Content Principles"' (2020) 53 *Comparative and International Law Journal of Southern Africa* 1 4.
[950] Recitals 7 and 13, GDPR.
[951] Recital 13, GDPR.

https://uwcscholar.uwc.ac.za/home

collection, analysis and monetisation of personal information, which are central aspects of this dissertation.

5.3.3.1 Selected principles

FIPs are central to GDPR and fundamental to the EU's approach to data protection. These data protection principles operate cumulatively and therefore each principle must be applied for the processing of personal information to be legitimate.[952] Compliance is achieved by the application of FIPs to how personal information is used in practise, rather than by following a set of prescriptive rules.[953] The responsibility for ensuring that the principles are applied rests with those who process the data.[954] South Africa adopts a similar approach in terms of POPIA. However, individuals in the US are responsible for protecting their own privacy.[955] At first glance, it appears like both South Africa and the EU may provide individuals with better protection compared to the US. It may be reasonable to make such an inference from the inclusion of a greater number of FIPS in data protection instruments, such as the GDPR and POPIA. However, a question that emerges, which is a follow-up to the questions posed above,[956] pertains to the role that these principles play in shaping a perception of personal data as a form of property. The GDPR has implemented selected FIPs, as summarised below.

5.3.3.1.1 Lawfulness, fairness and transparency

Article 5(1)(a) of the GDPR provides that personal information processing activities should be performed in a manner that is lawful, fair and transparent. In terms of recital 40, for the processing of personal information to be considered lawful,[957] it should be processed based on the consent of the data subject concerned or some other legitimate basis provided for in data

[952] Hoofnagle C, Van der Sloot B & Zuiderveen Borgesius F (2019) 76–8.

[953] Gallie A 'The General Data Protection Regulation – A Two–Year Retrospective' (22 May 2020) available at *https://www.lexology.com/library/detail.aspx?g=71abd6e1–83d6–4cf1–b807–fe6ef1565b6a* (accessed 4 March 2022).

[954] Hoofnagle C, Van der Sloot B & Zuiderveen Borgesius F (2019) 73. In contrast to the EU and South Africa, data subjects in the US are responsible for reading and evaluating privacy notices and making choices in the marketplace with respect to their personal data. Article 4(7) of the GDPR refers to those persons who, alone or jointly with others, determine the purposes and means of the processing of personal data as the 'controller'.

[955] See 4.7.2 above.

[956] See 4.2 above.

[957] Kuner C et al (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 314 explains that 'lawful' means that the data processing meets all the applicable legal requirements.

https://uwcscholar.uwc.ac.za/home

protection legislation. There are several grounds for lawful processing of personal information listed in art 6(1) of the GDPR.[958] Kuner et al state that lawful processing should also be understood with reference to conditions for lawful limitations of rights and freedoms in view of art 52(1) of the EUCFR.[959] Limitations, in terms of art 52(1), of the right to data protection may only be permitted if, first, such limitations respect the essence of the right to data protection, secondly, the processing of personal information pursues a legitimate purpose, and thirdly, is necessary and proportionate in a democratic society to achieve such purpose.[960]

Fair processing entails that personal information is not obtained or processed in an unfair manner, such as without the knowledge of the data subject or through deception.[961] Fairness involves data subjects' being able to access their data.[962] This is especially important in the context of big data, where smart devices and IoT are facilitating the proliferation of passive and indirect data collection without the data subject's knowledge and using such data to influence people's decision-making and behaviour.[963] Personal information may be monetised to the detriment of data subjects. The use of predictive analytics and machine learning places the data processor in a dominant position to exploit the data subject, and therefore Malgieri articulates the concept of fairness in the GDPR as 'the protection of individual vulnerabilities and the prevention of vulnerability exploitation, as consequences of significant power imbalance between individuals'.[964]

The principle of transparency requires that any party processing a data subject's personal information take appropriate measures to inform the data subject as to who will use the data and how it will be used.[965] Transparency means that the data subject should be informed before the processing commences, and the information should be readily available to data subjects during processing or following requests by data subjects for access to their information.[966] Felzmann et al state, with merit, that transparency is a prominent issue due to automated

[958] These grounds include obtaining the consent of the data subject; processing personal data that is necessary for the performance of a contract; processing is necessary to comply with a legal obligation; processing is necessary to protect the vital interests of the data subject; processing is necessary for the performance of a task carried out in the public interest; or it is carried out for the purposes of the legitimate interests of a party processing such data.

[959] Kuner C et al (2020) 314.

[960] European Union Agency for Fundamental Rights et al (2018) 42–3.

[961] Kuner C et al (2020) 314.

[962] C Bedir 'Contract law in the age of big data' (2020) 16 European Review of Contract Law 347 353.

[963] See 2.2.3 above.

[964] Malgieri G *The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation* (2020) 163.

[965] Article 12, GDPR; Recital 39, GDPR.

[966] European Union Agency for Fundamental Rights et al (2018) 120.

https://uwcscholar.uwc.ac.za/home

decision-making and will play a key role in fostering trust.[967] Trust in online services is identified as an essential factor in fulfilling the potential of the digital economy and encouraging economic growth and competitiveness.[968]

In comparison, POPIA requires that personal data ought to be processed lawfully.[969] Despite the wording being slightly different from that used in the GDPR, it is submitted that the intent of both the GDPR and POPIA are the same. However, the noticeable difference is that in the case of POPIA, such processing must not be done in a manner that infringes on the privacy of the data subject.[970] In chapter three, it was argued that privacy and data protection are two distinct concepts.[971] Therefore, since the GDPR does not associate lawful processing with safeguarding the privacy of the data subject, it is reasonable to infer that the concept of lawful processing under POPIA is narrower than under the GDPR. The implications are that data processing that does not affect the privacy interests of the data subject falls outside of s 9 of POPIA. This is particularly significant in cases where data processing leads to the commodification of personal data without necessarily affecting privacy concerns.[972] This supports the argument made in chapter three that POPIA does not envisage a situation in which personal data is treated as property.[973]

UNIVERSITY of the
WESTERN CAPE

5.3.3.1.2 Purpose limitation

The purpose limitation principle states that personal information must be collected for a specific, explicit, and legitimate purpose and may not be further processed in a way that is incompatible with the original purpose.[974] The data subject ought to be informed of the purposes of the data processing at the time of collection. Such processing may not be for undefined or unlimited purposes. The reason for which the data is processed must also be

[967] Felzmann H et al 'Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns' (2019) *Big Data and Society* 1 9. Felzmann et al contend that transparency under art 5 of the GDPR includes both a prospective and retrospective element, the former referring to individuals having to be informed data processing takes place and the latter referring to how and why a particular decision was reached.
[968] Reding (2012) 124.
[969] Section 9(a), POPIA.
[970] Section 9(b), POPIA.
[971] See 3.4 above.
[972] Privacy concerns in South Africa revolve around the right to be left alone.
[973] See 3.5 above.
[974] Article 5(1)(b), GDPR.

https://uwcscholar.uwc.ac.za/home

legitimate and should ensure a balancing of rights between those entitled to data protection and those who desire to process such data.[975]

Zarsky argues, correctly in my view, that the purpose limitation principle appears to clash with the kinds of uses that are so typical of the big data age and that involve methods and usage patterns not contemplated at the time of collection.[976] In chapter two, it was argued that opportunities for innovation and value creation lie in the re-use and secondary uses of personal information, that is, using data for purposes other than those for which it was initially collected.[977] By curtailing big data processing activities, innovation opportunities could diminish and adversely affect economic growth and competitiveness.

5.3.3.1.3 Data minimisation

The data minimisation principle provides that data must be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'.[978] The principles of data minimisation and purpose limitation are closely related. Data minimisation requires that only those categories of data relevant for a specific purpose should be processed.[979] According to Zarsky, data minimisation places an obligation on processors to limit their data collection and use only that which is needed.[980] He further argues that data minimisation will frustrate big data initiatives as they are dependent on analyses of large volumes of data to identify patterns and extract meaningful insights.[981] Moreover, data should not be stored for longer than is necessary to achieve the objectives of the processing operations.[982]

[975] Kuner et al (2020) 315.
[976] Zarsky T 'Incompatible: The GDPR in the age of big data' (2017) 47 *Seton Hall Law Review* 995 1005–7.
[977] See 2.3.4.5 above.
[978] Article 5(1)(c), GDPR.
[979] European Union Agency for Fundamental Rights et al (2018) 125.
[980] Zarsky T (2017) 1010.
[981] Zarsky T (2017) 1010–11.
[982] Kuner et al (2020) 317.

https://uwcscholar.uwc.ac.za/home

5.3.3.2 Lawful grounds for processing data

There can be no lawful processing of data without a legal justification.[983] The following sub-sections deal with those legal grounds that are deemed most relevant in the context of data-driven business models. Data-driven transactions require contracts between the data subject and the data processor to be concluded in order to process information. Therefore, the focus will be on consent as a basis for the processing of personal information,[984] the necessity of the processing for contract performance,[985] and the processing that is required for the data processor's legitimate interests.[986]

5.3.3.2.1 Consent

In a digital environment, data-driven business models are predominantly based on the processing of personal information obtained through consent.[987] Consent is seen as a key tool in allowing data subjects to retain some control over the processing of their personal information under EU data protection legislation.[988] Article 6(1)(a) provides that processing is lawful if 'the data subject has given consent to the processing of his or her personal information for one or more specific purposes'. Consent is defined as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to him or her'.[989] Companies that trade in personal information ought to ensure that consent is unambiguous, informed, including information about the commercial purpose of the data processing, free, and revocable.[990]

When establishing whether consent is 'freely given', it is important to evaluate whether the fulfilment of a contract is conditional on agreement for the processing of personal information

---

983 Voigt A & Von dem Bussche A *The EU General Data Protection Regulation (GDPR): A Practical Guide* (2017) 92; *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado* Joined Cases C-468/10 and C-469/10 ECLI:EU:C:2011:777 para 26. See also art 6(1)(a)–(f) of the GDPR.

984 Article 6(1)(a), GDPR.

985 Article 6(1)(b), GDPR.

986 Article 6(1)(f), GDPR.

987 EDPS (2017) para 56.

988 Lazaro C & Le Métayer D 'The control over personal data: True remedy or fairy tale?' (2015) 12 SCRIPTed 3 17–8; WP29 *Guidelines on Consent under Regulation 2016/679* (2018) 3.

989 Article 4(11), GDPR.

990 Janeček V & Malgieri G 'Commerce in data and the dynamically limited alienability rule' (2020) 21 *German Law Journal* 924 935. See also arts 7(1)–(4) of the GDPR.

https://uwcscholar.uwc.ac.za/home

that is not required for its performance.[991] When consent is packaged as a non-negotiable aspect of the terms and conditions, it is deemed not to have been freely provided.[992] For instance, we cannot consider a mobile photo editing app as freely given if it requires users to consent to the collection of their GPS location information for geo-tagging photographs and behavioural advertising.[993] A data subject must have the right to refuse or withdraw consent at any time without detriment.[994]

Detriment would generally occur when the data subject is placed at a disadvantage when refusing or withdrawing consent, or is coerced or intimidated into providing consent.[995] Pormeister states that the data subject should be informed of his right to withdraw consent before giving it, and the process to withdraw such consent should be as uncomplicated as possible.[996] As the withdrawal of consent takes effect from the moment it is withdrawn, the effectiveness of such a right may be rendered less effective in those instances when personal information has already been processed and monetised.[997] In such instances, it would be impractical for the withdrawal of consent to affect or undo any prior processing. It is submitted that the withdrawal of consent would only affect the lawfulness of subsequent processing.

Recital 43 of the GDPR provides that 'consent should not provide a valid legal ground for the processing of personal information in a specific case where there is a clear imbalance between the data subject and the controller…'. Information asymmetry or a data subject's lack of choice to use another service means that he is not in a position to refuse consent.[998] A lack of alternatives, especially if only 'free' online services are made available, suggests that consent has not been validly granted.[999] Bühler does not define freedom of choice as the availability of alternative services from other service providers but rather as the ability of a data subject to choose between two versions of a product or service, one requiring monetary payment and the

[991] Article 7(4), GDPR.
[992] WP29 (2018) 5.
[993] WP29 (2018) 6. See also Recital 42 of the GDPR.
[994] European Union Agency for Fundamental Rights et al (2018) 112.
[995] WP29 (2018) 10–1. For example, a data subject enjoys the full functionality of a mobile app provided the data subject grants the app permission to access location information. Should the data subject later refuse permission for the app to access his location information, detriment is clearly demonstrated if the app now only offers limited functionality.
[996] Pormeister K 'Informed consent to sensitive personal data processing for the performance of digital consumer contracts on the example of "23andMe "' (2017) 6 *Journal of European Consumer and Market Law* 17 19.
[997] EDPS (2017) para 69; See also art 7(3) of the GDPR.
[998] EDPS (2017) para 59.
[999] WP29 *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC* (2014) 47.

https://uwcscholar.uwc.ac.za/home

other relying on consent to use personal information.[1000] Bühler points out that consumers often have no choice but to consent to the processing of their personal information should they wish to use a certain device or access a service.[1001] The imbalance underscores the weaker bargaining power of the data subject in relation to the supplier of the service to either accept the terms or not conclude a contract, consequently affecting the autonomy of the data subject.[1002] In such instances, the provider of the service cannot rely on consent as a ground for processing the data, as the lack of choice renders any consent invalid.

Consent as a valid ground for processing in terms of POPIA mirrors, to a large extent, that which is stated in the GDPR.[1003] However, the requirement for consent to be given by 'clear and affirmative action' is absent from POPIA.

5.3.3.2.2 Contractual necessity

Article 6(1)(b) of the GDPR stipulates that 'processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract'. According to Voigt and Von dem Bussche, necessity must be determined by weighing the processing purposes and the contractual provisions in question.[1004] Necessity entails that processing ought to be reasonable and proportionate, and that personal information should be processed in the least intrusive manner.[1005] In *Schecke*, the Court held that limitations of data protection rights should only apply when strictly necessary and that the least intrusive measures to achieve the intended purpose should be employed.[1006] The European Data Protection Supervisor (EDPS) recommends the following factors be considered in assessing whether processing of personal information is necessary as contemplated in art 6(1)(b):[1007]

[1000] Bühler S 'Conditional consent as a valid legal ground for data processing – a misbelief?' (2019) *Freiburg Law Students Journal* 25 27.
[1001] Bühler S (2019) 25. Bühler cites the example of Netflix, the use of which is dependent on providing consent. See also EDPS (2017) 59.
[1002] Bedir C (2020) 351–52; Bühler S (2019) 26.
[1003] See ss 1 and 11(1)(a), POPIA.
[1004] Voigt A & Von dem Bussche A (2017) 102.
[1005] EDPS *Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects* (2019) para 25.
[1006] Joined Cases C 92/09 and C 93/09 ECLI:EU:C:2010:662 para 86.
[1007] EDPS (2019) para 33.

https://uwcscholar.uwc.ac.za/home

- nature of the service being provided to the data subject and its distinguishing characteristics;
- the rationale for the contract;
- essential elements of the contract; and
- the reasonableness of the envisaged processing that will take place to perform the contract.

If the contract cannot be fulfilled without the processing of personal information, then such processing is necessary.[1008] The Article 27 Working Group has clarified that the necessity requirement 'must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller'.[1009]

Janeček and Malgieri submit that art 6(1)(b) excludes the possibility of a contract being used as a legal basis for processing data for monetisation purposes.[1010] Bedir, on the other hand, proposes that the processing of personal information in data-driven business models may be required for the efficient functioning of contracts in which data subjects submit personal information in exchange for non-monetary goods or services.[1011] For example, should a data subject wish to use a smartphone app that reports on the local weather, the data subject may grant the app access to his location information in order for the app to process such data that is necessary for the purposes of providing a weather report.[1012] In these data-driven models, the data subject exchanges personal information to use the app. Robert and Smit state, with merit, that it would be difficult to argue that the personal information so provided would not be deemed necessary for the performance of the contract within the meaning of art 6(1)(b).[1013] Personal information, when used as a medium of exchange, could therefore potentially result in service providers requiring information as a condition to access services that are not strictly necessary for the performance of the contract.[1014]

[1008] Voigt A & Von dem Bussche A (2017) 102; Durovic M & Montanaro M 'Data protection and data commerce: Friends or foes?' (2021) 17 *European Review of Contract Law* 1 28.
[1009] WP29 (2014) 16–7.
[1010] Janeček V & Malgieri G (2020) 935.
[1011] Bedir C (2020) 348–49.
[1012] Helberger N, Zuiderveen Borgesius F & 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 1433.
[1013] Robert R & Smit L 'The proposal for a directive on digital content: A complex relationship with data protection law' (2018) 19 *ERA Forum* 159 168.
[1014] Robert R & Smit L (2018) 168.

https://uwcscholar.uwc.ac.za/home

The CJEU has been asked to rule on the issue of targeted adverts and the validity of collecting user data through such ways.[1015] Briefly, the facts are that Facebook asserts that its targeted advertisements are necessary and permitted by its terms of service, which constitute a contract between Facebook and its individual users.[1016] Prior to the GDPR coming into force, Facebook relied on users' consent to deliver targeted advertising; Facebook now contends that a contract between itself and the users is the basis for data processing.[1017] Facebook claims its terms of service require the company to collect data about its users and serve them targeted advertisements.[1018] Facebook further claims that the targeted advertisements enable the free use of the service.[1019] The litigation revolves around whether a user's (one-time) click on the 'yes' button relating to the processing of personal information represents consent or a contract. The CJEU must decide whether Facebook, by modifying the legal basis for its processing, undermines the stricter legal basis of consent by reinterpreting its services as contractual performance.[1020] Other issues that require clarification relate to Facebook's collection of data from 'Like' buttons and other online sources and the aspect of necessity with respect to the processing of personal information for behavioural advertising purposes.[1021] At the time of writing, the matter was still pending before the CJEU.

UNIVERSITY of the
WESTERN CAPE

It is significant to note that POPIA, in contrast, does not require processing to be necessary for a specific purpose.[1022] In light of the preceding paragraphs, this suggests that there is no impediment to the processing of personal information for the purposes of commodification, either through personal information being used as a medium of exchange or the monetisation of personal information through behavioural advertising. This further implies a lower level of protection for data subjects.[1023]

[1015] *Maximilian Schrems v Facebook Ireland Limited* (2021) Oberster Gerichtshof 6 Ob 56/21k (translation).
[1016] Paragraph 50.
[1017] Paragraphs 7–8.
[1018] Paragraph 53.
[1019] Paragraph 53.
[1020] Paragraph 54.
[1021] Paragraph 55. EDPS *Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects* (2019) paras 52–3 state as a general rule, the processing of personal information for behavioural advertising is not necessary for the performance of a contract for online services. However, personalisation of content could be expected with regard to some online services and may be considered necessary for the performance of the contract.
[1022] Roos A (2020) 18.
[1023] Roos A (2020) 18.

https://uwcscholar.uwc.ac.za/home

5.3.3.2.3 Legitimate interests

Legitimate grounds as a basis for processing is central to private sector processing.[1024] Article 6(1)(f) of the GDPR provides that 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal information…'. As an example, recital 47 of the GDPR provides that legitimate interests could exist 'where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller'. Legitimate interests as a legal ground for processing, however, have proved problematic in the context of monetisation of personal information.[1025]

According to the WP29, three tests should be taken into account when considering a legitimate interest as a basis for processing: the legitimacy of the interest in carrying out the processing; the necessity of the processing to achieve the intended purpose; and balancing the legitimate interests of controllers and third parties against the fundamental rights and interests of the data subject.[1026] For an interest to be legitimate, it must be lawful, sufficiently clear and specific, and represent a real and present interest.[1027] For example, a company that engages in online marketing and advertising activities is recognised as having a legitimate interest.[1028] This includes personalised or behavioural advertising.[1029]

However, the existence of a legitimate interest alone does not mean that the requirements for processing in terms of art 6(1)(f) are satisfied.[1030] Processing must be necessary, and it is deemed necessary if there is no less intrusive alternative to achieve the same purpose.[1031] Some scholars are sceptical that obtaining a monetary benefit from exchanging personal information would be regarded as adequate to fulfil the necessity test because profit may be obtained through less intrusive means, such as making the service accessible at a fee.[1032] It is agreed that

[1024] Kuner C et al (2020) 326.
[1025] Janeček V & Malgieri G (2020) 936.
[1026] WP29 (2014) 55. See also *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'* Case C-13/16 ECLI:EU:C:2017:336 paras 28–34.
[1027] WP29 (2014) 25.
[1028] Zuiderveen Borgesius F 'Personal data processing for behavioural targeting: Which legal basis?' (2015) 5 *International Data Privacy Law* 163 167.
[1029] Voigt A & Von dem Bussche A (2017) 103–4.
[1030] Zuiderveen Borgesius F (2015) 168.
[1031] WP29 (2014) 29. See also 5.3.3.2.2 above.
[1032] Janeček V & Malgieri G (2020) 936; Zuiderveen Borgesius F (2015) 169.

https://uwcscholar.uwc.ac.za/home

it is doubtful that the legitimate interest basis for processing alone in terms of the GDPR would provide sufficient grounds for data-monetisation practices such as behavioural advertising and intrusive profiling.[1033] It is submitted that this can be attributed to the fundamental rights-based approach that underpins the GDPR. As such, data monetisation practices are not likely to be recognised as legitimate grounds for processing personal data. On the other hand, the GDPR does not expressly preclude or permit personal data monetisation or its use as a medium of exchange, despite the EDPS having expressed an opinion on the matter. However, adopting a position that dismisses the commodification of personal data as not being a legitimate interest does not reflect everyday data practices. While the need to uphold dignity likely drives such an approach, the commodification of personal data is a global phenomenon rather than only a US one. The EU recognises this quandary and has implemented further legislative instruments to more effectively address these issues. This aspect will be discussed further below.[1034]

Given the lack of South African jurisprudence on the subject, it is reasonable to argue that South Africa would look to the GDPR for guidance to determine what 'legitimate interests' in the context of POPIA ought to be and how it should be dealt with.[1035] In light of the EU adopting alternative legal mechanisms, such as the Digital Content Directive, to deal with these data practices, South Africa is further hamstrung because it does not possess similar measures to confront the issue of commodification. Like the GDPR, POPIA does not explicitly prohibit or allow the monetisation of personal data or its use as a form of trade. Despite this apparent silence, data protection frameworks like the GDPR and POPIA facilitate the handling of personal data in a manner that resembles a property rights-oriented approach. The next section will delve into this aspect.

5.4 PROPERTY RIGHTS IN PERSONAL INFORMATION

The extensive discussions in the US concerning the idea of vesting property rights in personal information have largely driven parallel debates in the European context.[1036] Even though the property rights debate is seen primarily as providing an American solution to an American data protection problem, Purtova contends that the US debate presents valuable ideas for

[1033] See also Durovic M & Montanaro M (2021) 31.
[1034] See 5.5 below.
[1035] Burns Y & Burger-Smidt A *Protection of Personal Information: Law and Practice* 2 ed (2023) 114.
[1036] Lynskey O (2015) 233.

https://uwcscholar.uwc.ac.za/home

consideration from a European perspective.[1037] The creation of property rights in personal information may appear to be incompatible with a human rights-based approach to privacy; however, the EU system offers considerable leeway for a property rights model and appears to be more receptive to a property approach than the US system.[1038] Victor notes that although the EU data protection regulations do not explicitly establish property-like protections for personal information, they already incorporate the features outlined in Schwartz's hybrid model.[1039] This prompts an enquiry into whether a human rights-driven approach to privacy and the treatment of personal information as property can coexist. To address this question, the following sections examine aspects of the current EU data protection regime and the Digital Content Directive that could potentially promote the trade of personal information.

5.4.1 GDPR: Property-like entitlements

As a point of departure, Hazel mentions, importantly, that the GDPR does not 'reflect a policy judgment that property rights in personal information are normatively desirable', nor does it expressly grant property rights in such information.[1040] The GDPR aims to enhance data subjects' control of their personal information by providing them with rights such as the withdrawal of consent,[1041] the right to be forgotten,[1042] the right to data portability,[1043] and the right to object. [1044] Chapter three above discussed the advocacy of control as the leading paradigm for fostering self-determination and autonomy in personal information processing activities.[1045] Recital 7 of the GDPR emphasises control as a key component of the data protection framework, affirming that data subjects should have control over their personal information.

[1037] Purtova N (2009) 520.
[1038] Prins C *The Future of the Public Domain* (2006) 224.
[1039] Victor J (2013) 521. See also Hazel S 'Personal Data as property' (2020) 70 *Syracuse Law Review* 1055 1085 who states that: 'That Regulation is relevant here because it installs a property regime for personal data. The enactment of GDPR–and the proliferation of its approach–affirms that the gains from extending property rights in personal data are increasingly apparent.' See 4.10.1 above for a discussion of Schwartz's hybrid model.
[1040] Hazel S (2020) 1085–87. See also 5.3.3.2.3 above.
[1041] Article 7(3), GDPR.
[1042] Article 17, GDPR.
[1043] Article 20, GDPR.
[1044] Article 21, GDPR.
[1045] See 3.2.2 above.

https://uwcscholar.uwc.ac.za/home

The GDPR's efforts to enhance data subjects' control have led some scholars to conceptualise control in terms of property.[1046] Such control has been linked to the right to exclude, transfer, destroy, and use, all of which are central elements of property.[1047] This conception entails that property is defined as a 'bundle of rights' or entitlements rather than a specific object or thing.[1048] Cheneval states that these negative actions of property, specifically the ability to block interference from others, are already contained in the GDPR.[1049] The following sections demonstrate how the rights afforded by the GDPR could conceivably promote property rights in personal information.

5.4.1.1 Consent

As was previously mentioned, the consent mechanism provides an important tool for individuals to exert some control over the processing of their personal information.[1050] Purtova, rightly, comments that 'nothing establishes the relationship of control between an individual and personal information—characteristic of property—as strongly and unequivocally as the consent rule does …'.[1051] In other words, the data subject has the discretion to allow another party to use his or her personal data or exclude others from using it.

According to Boerding, accessibility and use of personal information are tied to explicit consent, with the resultant data ownership being determined by the GDPR.[1052] This suggests that when processing personal information is conditional on consent, data ownership should be allocated to the data subject, who will have the authority to determine how his personal information may be used. Victor argues that the GDPR is predicated on the assumption that

---

[1046] Victor J (2013) 522 remarks that the protection mechanisms in the GDPR function like regulated property schemes. Pearce H (2018) 198–98 notes that the notion of data protection as the ability to control personal data has evolved into an idea as the ability of individuals to 'own' their personal data. De Hert P et al 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services' (2018) *Computer Law and Security Review* 193 201 in referring to the relationship between the data subject and personal data uses the expression 'data relating to him or her'.

[1047] Hazel S (2020) 1088.

[1048] Hohfeld W 'Fundamental legal conceptions as applied in judicial reasoning' (1917) 26 *Yale Law Journal* 710 746–47; Del Rosario L 'On the propertization of data and the harmonization imperative' (2022) 90 *Fordham Law Review* 1699 1707.

[1049] Cheneval F (2018) 5.

[1050] See 5.3.3.2.1 above. WP29 (2018) 3 states that where consent is properly obtained, it is a 'tool that gives data subjects control over whether or not personal data concerning them will be processed'.

[1051] Purtova N *Property Rights in Personal Data* (published PhD thesis, Tilburg University, 2011) 193.

[1052] Boerding A et al 'Data ownership -A property rights approach from a European perspective' (2018) 11 *Journal of Civil Law Studies* 323 366.

https://uwcscholar.uwc.ac.za/home

personal information is a commodity that can be exchanged and that the property entitlement belongs to the data subject, which can be 'licensed' to a data processor to use by way of consent.[1053]

It is evident that the issue of ownership also features prominently in the EU discourse. In contrast to the US, which focuses primarily on property rules to determine absolute ownership in order to facilitate market exchanges,[1054] the EU discussion on ownership revolves around a bundle of rights approach. The bundle of rights approach is based on the idea that property comprises not only the right of ownership but also the rights to alienate and exclude.[1055] Therefore, consent is only one aspect of ownership, meaning that one individual's rights and entitlements can be limited by the rights and interests of others. Depending on the context, property can be defined with reference to any specific bundle of rights, including the rights of others. As a result, property is defined in relation to the rights to use it, not the object. As mentioned in chapter four, this understanding of property is especially applicable in the South African context because s 25 of the Constitution focuses on safeguarding property, rather than ownership.[1056] The next chapter will delve into this aspect.

UNIVERSITY of the
WESTERN CAPE

5.4.1.2 The right to data portability

The GDPR introduces the right to data portability which provides that:[1057]

> 'The data subject shall have the right to receive the personal information concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal information have been provided….'

It needs to be pointed out that although POPIA does not expressly refer to a right to data portability, it makes provision for data subjects to request that personal information be

[1053] Victor J (2013) 515 524. See also Bedir C (2020) 360.

[1054] See 4.9.3 above.

[1055] Hohfeld W 'Fundamental legal conceptions as applied in judicial reasoning' (1917) 26 *Yale Law Journal* 710 746–47; Baron J (2012) 384–90; Del Rosario L (2022) 1707.

[1056] See 4.9.3 above.

[1057] Article 20(1), GDPR. Li W *Data Portability as a New Means of Data Protection? Examining the Right to Data Portability in the EU General Data Protection Regulation* (unpublished PhD thesis, University of Edinburgh, 2019) 8 states that while data portability has often been used in the areas of competition and consumer welfare, its use as a data protection mechanism is a recent innovation.

https://uwcscholar.uwc.ac.za/home

transmitted to another automated processing system.[1058] Arguably, it may be inferred that POPIA does provide data subjects with a right to data portability, but unlike the GDPR, it fails to outline the conditions for the transfer of data and the obligations of the responsible party. Moreover, this forms part of a processing condition rather than a right, and it is therefore reasonable to argue that the GDPR offers a higher standard of protection in this regard. The inclusion of such a right in the GDPR demonstrates an appreciation on the part of EU policymakers that processing may be motivated by commercial interests. It further highlights that data protection is no longer solely focused on the right to privacy, as is the case with POPIA and the now repealed Data Protection Directive.

According to De Hert et al, the right to portability comprises three different elements (1) the right of the data subject to receive his personal information without hindrance, (2) the right to transmit personal information without hindrance and (3) the right to have the personal information transmitted directly from one service provider to another where technically feasible.[1059] Data portability aims to strengthen the data subjects' control over their personal information.[1060] The objective is to empower data subjects with a useful and effective means to move, copy, or transmit datasets containing their personal information from one IT environment to another.[1061] Aside from enhancing the information self-determination of data subjects, data portability is expected to play a key role in facilitating the free flow of information in terms of the EU's DSM by potentially reducing costs for consumers wishing to switch service providers and thereby prevent lock-ins, lowering barriers of entry, promoting competition so that new entrants may gain access to data and encouraging the development of new products and services.[1062]

A data subject is entitled to exercise the right to portability only when personal information is processed by automated means on the grounds of consent or pursuant to a contract to which

[1058] Burns Y & Burger-Smidt A (2023) 292; Section 14(6)(d), POPIA.

[1059] De Hert P et al (2018) 197. See also WP29 *Guidelines on the Right to Data Portability* (2017) 5.

[1060] Recital 68 of the GDPR provides that '[t]o further strengthen the control over his or her own data…, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller'.

[1061] WP29 (2017) 4. Li W *Data Portability as a New Means of Data Protection* (2019) 83 states that portability enables a new paradigm of control called 'redistributive control' which directly facilitates the economic empowerment of individuals.

[1062] EC *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European Interoperability Framework - Implementation Strategy* (2017) 12–3.

https://uwcscholar.uwc.ac.za/home

the data subject is a party.[1063] Data portability will not apply when processing is based on any of the other grounds mentioned in art 6(1).[1064] According to the WP29, only personal information that is 'actively and knowingly provided by the data subject' or 'observed data provided by the data subject by virtue of the use of the service or the device', such as search history or location data, will be subject to data portability.[1065] Inferred data, insights and data derived through analytical means are excluded from the scope of the right to data portability.[1066]

Article 20 of the GDPR does not clearly articulate how the right to data portability can assist the data subject in achieving control over their personal information.[1067] However, Ursic believes that some of the data portability objectives that are instrumental to privacy and data protection can be distilled from the GDPR as a whole, such as strengthening control over data sharing and establishing control over the reuse of personal information.[1068]

UNIVERSITY of the
WESTERN CAPE

5.4.1.2.1 Control over data sharing

Data portability grants data subjects the ability to determine how their personal information ought to be shared and reused.[1069] This ability constitutes a form of control, the exercise of which is not limited in any way by law to only certain types of socially beneficial activities or goals.[1070] Data portability may be implemented in two ways:[1071]

(i) transmitting the entire dataset; or

(ii) providing a tool that allows for the extraction of relevant data for transmission.

[1063] Articles 20(1)(a) and (b), GDPR.

[1064] This includes arts 6(1)(c), (d) and (e) of the GDPR. For example, personal information processed for the purposes of combatting money laundering and financial crimes is not subject to data portability.

[1065] WP29 (2017) 10.

[1066] WP29 (2017) 10.

[1067] Ursic H 'Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control' (2018) 15 *SCRIPTed* 42 58. Li W *Data Portability as a New Means of Data Protection* (2019) 41–2 comments that the underlying rationale for introducing data portability 'represents a new opportunity for personal data flows from systems exclusively controlled by organisations to those centred on users'.

[1068] Ursic H (2018) 59 explains that other objectives, such as enabling a better understanding of personal data flows, facilitating the development of personality, and enhancing equality, can also be extracted from the text.

[1069] WP29 (2017) 6.

[1070] Graef I, Husovec M & Purtova N 'Data portability and data control: Lessons for an emerging concept in EU law' (2018) 19 *German Law Journal* 1359 1369 describe this power as 'purpose-agnostic'.

[1071] WP29 (2017) 16.

https://uwcscholar.uwc.ac.za/home

Ursic submits, with merit, that the second option may be preferable as it allows only a defined set of information to be transmitted, therefore promoting control and ensuring that the receiving party receives only that data that is necessary to fulfil a specific activity or task.[1072] This approach helps reduce privacy concerns by enabling the delivery of only relevant data in response to the data subject's request, while ensuring that any data processing adheres to the concept of data minimisation.[1073]

5.4.1.2.2 Control over (re-)uses of personal information

Data portability enables a data subject to port personal information from one processing system to another, making it available for reuse elsewhere. Enhancing control over subsequent uses of personal information can potentially enable individuals to use such data to create value.[1074] According to Li, the right to portability places data subjects in the role of data controllers, allowing them to transfer their data to other systems of their choice and benefit from its reuse.[1075] The EDPS endorses the view that companies should not benefit exclusively from the secondary uses of personal information but that 'they should be prepared to share the wealth created by the processing of personal information with those individuals whose data they process'.[1076] Data portability will improve control over data reuse if it is supported by a functional infrastructure, such as providing data subjects with personal information stores, privacy dashboards, or personal information management software to manage access and the processing of personal information by controllers.[1077]

5.4.1.2.3 Data portability and property rights

De Hert et al point out that the GDPR, when referring to the relationship between personal information and data subjects, generally uses the expression 'data relating to him or her'.[1078]

[1072] Ursic H (2018) 60.
[1073] Article 5(1)(c), GDPR.
[1074] Ursic H (2018) 60.
[1075] Li W *Data Portability as a New Means of Data Protection* (2019) 62.
[1076] EDPS *Meeting the Challenges of Big Data: A Call for Transparency, User Control, Data Protection by Design and Accountability* (2015) 12–3.
[1077] Ursic H (2018) 61.
[1078] De Hert P et al (2018) 201. Conducting a search using the Find function in Adobe Reader reveals one result for the expression 'his or her own data' and one result for 'their own data', while there is a combined total of 16 results for the expressions 'data relating to him or her' and 'data concerning him or her'.

https://uwcscholar.uwc.ac.za/home

However, in recital 68 of the GDPR, reference is made to 'his or her own data'. Given that the EU views data protection as a fundamental right based on the values of dignity, individuality, and self-determination, the use of such terminology in a data protection context seems peculiar. De Hert et al state that the reference to 'own data' is related to the idea of control and that the right to data portability is 'an essential element towards empowerment of data subjects and a first step to an idea of data subjects' default ownership of their personal information'.[1079]

Hazel associates the right to portability with the transfer element of property.[1080] By placing the data subject in a position where he can make decisions about further processing and access, the right to data portability goes beyond mere consent and can be seen as another step towards data ownership.[1081] The EDPS, in recognising that data portability could potentially enable both businesses and individuals to benefit from the application of big data analytics to personal information and thereby redress economic imbalances, holds that the right to data portability will allow data subjects to benefit from the value created by their use of their personal information and licence their data for further use to third parties in exchange for services or cash value.[1082] Consequently, it seems that the EDPS has departed from its earlier position opposing the commodification of personal information.[1083] This is significant because it seems to suggest that there is a receptiveness to consider the idea that personal information may be seen as a commodity that can be transferred from one party to another. Moreover, the use of the word 'licence', typically used in the field of intellectual property law, envisages a situation where a person or party is granted the right to use property belonging to another.

5.4.1.3 The right to erasure (right to be forgotten)

Article 17 of the GDPR makes provision for a right to erasure or the 'right to be forgotten' as it is also known.[1084] The right to be forgotten was first recognised in 2014 in *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González (Google Spain)*.[1085] The CJEU was called upon to give guidance concerning the interpretation

[1079] De Hert P et al (2018) 201.
[1080] Hazel S (2020) 1089.
[1081] Boerding A et al (2018) 332.
[1082] EDPS (2015) 13.
[1083] See 5.2 above.
[1084] Hoofnagle C, Van der Sloot B & Zuiderveen Borgesius F (2019) 90 comment that the use of the phrase 'right to be forgotten' is regrettable since 'people cannot require others to forget them'.
[1085] Case C-131/12 ECLI:EU:C:2014:317.

https://uwcscholar.uwc.ac.za/home

of the right to deletion of data as outlined in art 12 of the Data Protection Directive.[1086] The CJEU held that EU data protection law gives data subjects the right to ask controllers, in this instance, search engines like Google, to erase information and links in certain results for queries related to a person's name, taking into account whether such information appears 'inaccurate, inadequate, irrelevant, or excessive'.[1087] The CJEU also aimed to balance the rights to privacy and data protection of the data subject against the public's legitimate interests in accessing information.[1088] Kuner et al point out that while *Google Spain* requires a search engine operator to remove links to the web page containing irrelevant or outdated personal information about the data subject, the web page itself may still be accessible using other search criteria, and therefore the overall effect of the decision is to reduce its 'public impact' or online presence and remove it from the 'active memory' of the Internet.[1089]

In terms of art 17(1) of the GDPR, '[t]he data subject shall have the right to obtain from the controller the erasure of personal information concerning him or her without undue delay and the controller shall have the obligation to erase personal information without undue delay…'.[1090] Some scholars state that the right to be forgotten is an elaboration of an already existing right that is given more prominence in the GDPR as an instrument for data subjects to retain some control over their personal information.[1091] Article 17 of the GDPR develops the right to deletion of data outlined in art 12 of the Data Protection Directive by aiming to address more effectively the privacy and dignitary harms associated with the online sharing of personal information.[1092] According to Forde, the right to be forgotten reinforces personal autonomy by affording the data subject more control over information from the past, which may negatively impact their future identity, and is a necessary response to the privacy concerns occasioned by technological innovation.[1093] Voigt and Von dem Bussche state, with merit, that the right to be forgotten is especially useful to data subjects in an online environment.[1094]

[1086] Case C-131/12 ECLI:EU:C:2014:317 para 20. Article 12 of the Data Protection Direction is the forerunner of art 17 of the GDPR.

[1087] Case C-131/12 ECLI:EU:C:2014:317 para 70.

[1088] Case C-131/12 ECLI:EU:C:2014:317 para 81.

[1089] Kuner C et al (2020) 479.

[1090] See also art 17(3)(a)–(e) of the GDPR for a list of exceptions when the right to be forgotten will not apply.

[1091] Walters R, Trakman L & Zeller B *Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches* (2019) 61–2; Kuner C et al (2020) 477.

[1092] Rubinstein I 'Big data: The end of privacy or a new beginning?' (2013) 3 *International Data Privacy Law* 74 80. The shortcomings of the Data Protection Directive were pointed out in 5.3.2 above.

[1093] Forde A 'Implications of the right to be forgotten' (2015) 18 *Tulane Journal of Technology and Intellectual Property* 83 89–90.

[1094] Voigt A & Von dem Bussche A (2017) 161.

https://uwcscholar.uwc.ac.za/home

The right to be forgotten, as articulated in the GDPR, will only be available to the data subject in the following circumstances:[1095]

- the personal information collected is no longer necessary in relation to the processing purposes;[1096]
- the data subject withdraws consent on which the processing is based according to art 6(1)(a) or art 9(2)(a);[1097]
- there are no overriding legitimate ground(s) for the processing or the data subject objects to the processing;[1098]
- data processing took place unlawfully;[1099]
- there is a legal obligation to erase personal information in compliance with legislation;[1100] and
- personal information has been collected in relation to the offer of information society services referred to in art 8(1).[1101]

The grounds for exercising the right with respect to arts 17(1)(a), (b) and (d) assume a lack of a basis for the processing of data, whereas no such assumption is made with respect to the remaining three grounds.[1102] The data subject is obliged to specify which provision under art 17(1) he is relying on and bears the burden of proof in those instances where it is claimed that no basis for the data processing exists.[1103] The data subject only has the right to object to data processing that is based on a contract or other legal basis.[1104] In such circumstances, processing must stop unless the controller can demonstrate compelling legitimate grounds for continued processing that override the rights of the data subject, thereby shifting the burden of proof to the controller.[1105]

[1095] Article 17(1), GDPR.
[1096] Article 17(1)(a), GDPR.
[1097] Article 17(1)(b), GDPR.
[1098] Article 17(1)(c), GDPR.
[1099] Article 17(1)(d), GDPR.
[1100] Article 17(1)(e), GDPR.
[1101] Article 17(1)(f), GDPR.
[1102] Kuner C et al (2020) 481.
[1103] Voigt A & Von dem Bussche A (2017) 159. For example, if the data subject can show that processing is no longer lawful because consent has been withdrawn, the controller must cease processing and cannot continue on alternative grounds. See also recital 65 of the GDPR.
[1104] Article 21(1), GDPR.
[1105] Article 21(1), GDPR; EDPS *Guidelines 5/2019 on the Criteria of the Right to Be Forgotten in the Search Engines Cases under the GDPR (Part 1)* (2019) 8.

https://uwcscholar.uwc.ac.za/home

When the right to erasure is successfully invoked by the data subject and any personal information has been made public, the controller must take reasonable steps to inform other controllers who have processed the data to delete all links, copies and replications thereof.[1106] In doing so, the original controller's obligation to inform others shall take into consideration the available technology, technological measures, and implementation costs to comply with a request for erasure.[1107] The right to be forgotten therefore encompasses the deletion of personal information and abstaining from further dissemination of such data.[1108]

5.4.1.3.1 Right to erasure and property rights

Successfully exercising the right to be forgotten under art 17(2) of the GDPR would entail one controller having to inform other controllers that the personal information of the data subject must be erased.[1109] According to some scholars, erasure resembles the right to destroy, which is an essential feature of property.[1110] Boerding et al state that the 'individual is granted a power of exclusive disposition concerning the processing of personal information that is – to some extent – comparable with the power of the owner over his property'.[1111]

By exercising the right to erasure, the data subject would effectively be invoking such a right against every controller in possession of his personal information. This right aligns with the property rules outlined by Schwartz in his hybrid inalienability model, in which a use-transferability restriction is imposed on any subsequent processing of personal information by third parties; that is, 'the burden of a property right "runs with the asset"'.[1112] Victor states, with merit, that 'third-party data users would be bound to respect the data subject's exercise of her right to be forgotten or risk incurring sanctions under the Regulation'.[1113] The right to erasure demonstrates how property rights can exclude others from processing the personal

[1106] Article 17(2), GDPR.
[1107] Article 17(2), GDPR; Recital 66, GDPR.
[1108] Harbinja E 'Does the EU data protection regime protect post-mortem privacy and what could be the potential alternatives?' (2013) 10 *SCRIPTed* 19 33–4.
[1109] Voigt A & Von dem Bussche A (2017) 163 opine that such an obligation is limited to reasonable steps and does not entail a comprehensive exercise to inform other controllers.
[1110] Harbinja E (2013) 34; Hazel S (2020) 1089.
[1111] Boerding A et al (2018) 331.
[1112] See 4.10.1 above for a discussion of Schwartz's hybrid inalienability model.
[1113] Victor J (2013) 524–25.

https://uwcscholar.uwc.ac.za/home

information to which the right pertains. This power to 'exclude' represents a negative dimension or non-market function of property rights.[1114]

5.5 DIGITAL CONTENT DIRECTIVE

The EU has identified the DSM as a key pillar to boost the region's digital economy by ensuring 'better access for consumers and businesses to online goods and services across Europe'.[1115] The DSM strategy recognises the supply of digital content and services as a key focus area with strong growth potential.[1116] One of the DSM's key strategic goals is to eliminate barriers to cross-border online activity and prevent unfair discrimination against consumers and businesses when trying to access content or purchase goods or services online.[1117] However, member states' differing consumer protection and contract laws discourage cross-border e-commerce, preventing consumers from benefiting from the full range of online offerings and competitive prices,[1118] while businesses conducting cross-border online transactions face increased costs.[1119] Therefore, the introduction of harmonised, coherent contract rules at the EU level to regulate cross-border online trade is necessary to increase consumer trust and legal certainty for businesses in the DSM.[1120]

In this regard, the introduction of the Digital Content Directive is significant as it seeks to regulate contracts for the supply of digital content and services by ensuring 'a high level of consumer protection, in order to achieve a genuine DSM, increase legal certainty and reduce transaction costs…'.[1121] Moreover, the Digital Content Directive is relevant for the purposes of this dissertation because it regulates, among other things, the so-called 'free' business

---

[1114] Boerding A et al (2018) 331.

[1115] EC *Impact Assessment: Accompanying the Document Proposals for Directives of the European Parliament and of the Council (1) on Certain Aspects Concerning Contracts for the Supply of Digital Content and (2) on Certain Aspects Concerning Contracts for the Online and Other Distance Sales of Goods* (2015) 4. See also 5.2 above.

[1116] EC *Contracts for the Supply of Digital Content and Online and Other Distance Sales of Goods* (2015) 5.

[1117] EC *A Digital Single Market Strategy for Europe* (2015) 4. Discrimination can be based on nationality, residence or geographical location.

[1118] EC *A Digital Single Market Strategy for Europe* (2015) 4.

[1119] EC *Impacts of Fully Harmonised Rules on Contracts for the Sales of Goods Supplementing the Impact Assessment Accompanying the Proposal for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Online and Other Distance Sales of Goods* (2017) 8–9.

[1120] EC *Contracts for the Supply of Digital Content and Online and Other Distance Sales of Goods* (2015) 5; EC *Impacts of Fully Harmonised Rules on Contracts for the Sales of Goods Supplementing the Impact Assessment* (2017) 11.

[1121] Recital 3, Proposal for a Digital Content Directive.

https://uwcscholar.uwc.ac.za/home

models involving the exchange of personal information.[1122] The following section looks at the Digital Content Directive in relation to the exchange of personal information.

5.5.1 Personal information as counter-performance

Metaphors like 'the new oil' or 'the new currency' are frequently used to highlight the significance of personal information in the digital economy.[1123] Exchanging personal information for goods and services is a well-established phenomenon.[1124] Versaci comments that the processing of personal information can create economic value.[1125] Companies benefit from the monetisation of personal data, and consumers benefit from tailored services and the greater availability of free content.[1126] Eggers, Hamill and Ali state, with merit, that '[p]ersonal data has an economic value that can be bought, sold and traded'.[1127] These characteristics fit the notion of currency, which is something that can serve as a medium of exchange, be 'cashed out' for goods or services, be used to settle debts or store value for future use.[1128]

It is significant to note that the Proposal for a Digital Content Directive envisages personal information having 'a value comparable to money'.[1129] It uses the term 'counter-performance' in relation to the exchange of personal information for digital content.[1130] Article 3(1) of the Proposal for a Digital Content Directive reads:

[1122] Recital 24, Proposal for a Digital Content Directive. De Franceschi A 'Personal data as counter-performance' in Senigaglia R, Irti C & Bernes A (eds) *Privacy and Data Protection in Software Services, Services and Business Process Reengineering* (2022) 59 distinguishes two types of personal data based business models, namely (1) the provision of personal data and the consent to its processing in exchange for the use of a service, such as, Facebook or Google, and (2) the provision of a basic version of service which does not require monetary payment, as well as a premium version of the service that requires a monetary counter-performance, like Dropbox and LinkedIn.

[1123] Kuneva M 'Roundtable on online data collection, targeting and profiling' (31 March 2009) *https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156* (accessed 16 March 2020); Versaci G 'Personal data and contract law: Challenges and concerns about the economic exploitation of the right to data protection' (2018) 14 *European Review of Contract Law* 374 377.

[1124] Langhanke C & Schmidt-Kessel M 'Consumer data as consideration' (2015) 4 *Journal of European Consumer and Market Law* 218 219.

[1125] Versaci G (2018) 376.

[1126] Kelly R & Swaby G 'Consumer protection rights and "free" digital content' (2017) 23 *Computer and Telecommunications Law Review* 165 166.

[1127] Eggers W, Hamill R & Ali A 'Data as the new currency: Government's role in facilitating the exchange' (2013) 13 *Deloitte Review* 18 19.

[1128] Eggers W, Hamill R & Ali A (2013) 21; Purtova N (2017) 70.

[1129] Recital 13, Proposal for a Digital Content Directive.

[1130] Recital 13, Proposal for a Digital Content Directive. The payment of money is an alternative counter-performance to personal data.

https://uwcscholar.uwc.ac.za/home

> 'This Directive shall apply to any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal information or any other data.'

Despite opposition to the idea that personal information can function as counter-performance,[1131] it will suffice for the purposes of this dissertation to state that such exchange will nevertheless involve consumer protection considerations.[1132] In this regard, Narciso asserts that consumers who provide personal information as a counter-performance to acquire goods ought to be entitled to the same level of consumer protection as those who pay money.[1133] It is submitted that Narciso recognises the economic value that is being exchanged. The next section explores the contentious issue of language usage in the Proposal for a Digital Content Directive, specifically in relation to the idea of personal information functioning as counter-performance.

5.5.2 Convergence between personal information as counter-performance and the human rights foundations of data protection

UNIVERSITY of the
WESTERN CAPE

The concept of personal information as counter-performance appears to be at odds with EU data protection law. Custers and Malgieri suggest that paying with personal information could be understood as paying with informational privacy.[1134] On the surface, such a notion appears to be irreconcilable with the EUCFR and the GDPR because the right to data protection is a fundamental right and therefore inalienable.[1135] This perspective aligns with the EDPS's stance, which maintains that personal information is a fundamental right and not a commodity.[1136] The right to data protection implicates personality interests and therefore could be considered an

[1131] See 5.5.2 below.

[1132] Consumer protection considerations are beyond the scope of this dissertation.

[1133] Narciso M '"Gratuitous" digital content contracts in EU consumer law' (2017) 6 *Journal of European Consumer and Market Law* 198 205.

[1134] Custers B & Malgieri G (2022) 1–2. Custers and Malgieri do proceed, however, to clarify that 'payment' in such a context is fundamentally different from its traditional meaning because personal information cannot be owned, and therefore cannot be used as payment.

[1135] Custers B & Malgieri G (2022) 4. Recital 1 of the GDPR provides that: 'The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') … provide that everyone has the right to the protection of personal data concerning him or her.'

[1136] EDPS (2017) para 14.

https://uwcscholar.uwc.ac.za/home

impediment to the commodification of personal information.[1137] In this regard, the EDPS asserts:[1138]

> 'There might well be a market for personal information, just like there is, tragically, a market for live human organs, but that does not mean that we can or should give that market the blessing of legislation. One cannot monetise and subject a fundamental right to a simple commercial transaction, even if it is the individual concerned by the data who is a party to the transaction.'

The EDPS further opines that introducing an explicit possibility to use personal information as counter-performance interferes with art 8 of the EUCFR and data protection legislation.[1139] Despite the fact that consumers do, in fact, exchange personal information for digital content and services, the Digital Content Directive, in line with the EDPS's position and in contrast to the Proposal for a Digital Content Directive, rejects any notion that personal information could be considered a commodity.[1140] The Digital Content Directive does not use the terms 'counter-performance' and 'in exchange' in relation to the provision of personal information to obtain goods and services.[1141] As a result, art 3(1) of the Digital Content Directive provides that:

> 'This Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal information to the trader, except where the personal information provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose.'

De Franceschi states that the Digital Content Directive aims to adopt a 'softer' formulation than the Proposal for a Digital Content Directive.[1142] This approach by the Digital Content Directive attempts to dispel any notion that it encourages the commodification of personal

[1137] Article 8, EUCFR.
[1138] EDPS (2017) para 17.
[1139] EDPS (2017) para 20.
[1140] Recital 24, Digital Content Directive.
[1141] A search using the Find function in Adobe Acrobat for the term 'counter-performance' displays no results.
[1142] De Franceschi A '*Personal data as counter-performance'* (2022) 62.

https://uwcscholar.uwc.ac.za/home

information.[1143] However, as De Hert and Sajfert correctly point out, the Digital Content Directive contradicts itself by explicitly rejecting the notion of personal information as a commodity, yet digital content can be supplied against the provision of personal information.[1144] Moreover, the concept of 'price' as defined in art 2(7) of the Digital Content Directive encompasses not only money but also a digital representation of value that can be exchanged for digital content. De Franceschi submits, and justifiably so, that in the context of the digital economy, a digital representation of value could include the provision of personal information.[1145] Efroni concludes, with merit, that this attempt to downplay any commercial aspects by removing phrases such as 'counter-performance' amounts to a semantic rather than a substantive alteration.[1146]

Despite these exclusions, it is argued that this clearly demonstrates an awareness and an appreciation of the commodification of personal data. If this were not the case, there would be no need to address it at all in the Digital Content Directive. It is also submitted that a distinction must be made between the fundamental right to data protection and the personal data that is the subject of protection. While a fundamental right is inalienable, the personal data itself may be the object of a commercial transaction. In other words, the exchange of personal data does not necessarily affect the individual's fundamental right to data protection.

Another relevant aspect of the interaction between the Digital Content Directive and the GDPR is that the GDPR will prevail in the event of a conflict between the two regimes regarding the processing of personal information.[1147] The two regimes are expected to operate concurrently.[1148] However, the data protection rules dictate the conditions under which personal information may be processed, including those instances relating to contracting under the Digital Content Directive for goods and services.[1149] Consequently, any processing of personal information under the Digital Content Directive must comply with the requirements

[1143] Efroni Z 'Gaps and opportunities: The rudimentary protection for "Data-Paying Consumers" under new EU consumer protection law' (2020) 57 *Common Market Law Review* 799 805.

[1144] De Hert P & Sajfert J 'Regulating Big Data in and out of the Data Protection Policy Field: Two Scenarios of Post-GDPR Law-Making and the Actor Perspective' (2019) 5 *European Data Protection Law Review* 338 346. See also Recital 24, Digital Content Directive.

[1145] De Franceschi A '*Personal data as counter-performance'* (2022) 63.

[1146] Efroni Z (2020) 805.

[1147] Article 3(8), Digital Content Directive.

[1148] Langhanke C & Schmidt-Kessel M (2015) 219–20 refer to two layers of protection. A consumer under the Digital Content Directive and a data subject under the GDPR are one and the same, as is a data controller in terms of data protection principles and a trader under the Digital Content Directive.

[1149] Bedir C (2020) 350. See also Efroni Z (2020) 805. Recital 48 of the Digital Content Directive provides that a contract for the supply of digital content must conform to the data protection principles contained in the GDPR.

https://uwcscholar.uwc.ac.za/home

for the lawfulness of the processing of personal information contained in Articles 6(1)(a) and (b) of the GDPR,[1150] such as consent.

If consent forms the basis for contract formation, it follows that withdrawing consent should also have contractual consequences. The right to erasure and the withdrawal of consent as provided for in the GDPR are fully applicable to contracts concluded under the Digital Content Directive.[1151] The lawfulness of any processing performed prior to withdrawal will not be affected by such withdrawal.[1152] If, however, no other grounds exist for the continued processing of personal information by the trader, then it must be deleted.[1153] Contracts which aim to restrict or limit these fundamental rights are not valid.[1154] Exercising a right to withdraw does not constitute a breach of contract, nor does it provide the trader with a claim for damages.[1155] The consumer has a right to data portability upon the termination of a contract for the supply of digital content.[1156]

Given that the two legal regimes may be in force simultaneously, there is potential for conflict because data collection and processing in terms of the GDPR must, from the outset, have a specific purpose that covers the entire contractual relationship between the parties.[1157] According to Efroni, in many cases, the processing of personal information provided as counter-performance may not comply with the necessity requirement for contract performance as articulated in art 7(4), and therefore a strict interpretation of the GDPR would frequently invalidate the consent given under the Digital Content Directive.[1158] This is because counter-performance implies that the trader can extensively process the supplied personal information to derive benefits or generate revenue. The withdrawal of consent means that the trader will be deprived of the economic value of the personal information that formed part of the contractual arrangement between the parties.[1159]

[1150] De Franceschi A '*Personal data as counter-performance'* (2022) 64. Articles 6(1)(a) and (b) provide for specific authorisations to process personal data, either by the data subject or by law. Articles 6(1)(c)–(f) provide for processing when public interest makes this necessary. See also 5.3.3.2 above.

[1151] Recital 39, Digital Content Directive.

[1152] Article 7(3), GDPR.

[1153] Bedir C (2020) 359.

[1154] Kull I 'Withdrawal from the consent to process personal data provided as counter-performance: contractual consequences' (2020) 13 *Journal of the University of Latvia Law* 33 44.

[1155] Langhanke C & Schmidt-Kessel M (2015) 222.

[1156] Li W *Data Portability as a New Means of Data Protection* (2019) 93.

[1157] Bedir C (2020) 357–58. See also recital 39 of the GDPR.

[1158] Efroni Z (2020) 806. See also De Franceschi A '*Personal data as counter-performance'* (2022) 64.

[1159] Kull I (2020) 44.

https://uwcscholar.uwc.ac.za/home

5.6 CONCLUSION

The EU data protection framework guarantees individuals the fundamental right to data protection. The GDPR, which implements several principles to ensure the fair and lawful processing of personal information to safeguard data subjects' human dignity and promote their fundamental rights and freedoms, demonstrates how highly regulated the processing of personal information is. In comparison to POPIA, the GDPR offers data subjects a higher level of data protection with the inclusion of new rights such as portability and erasure.

Data protection as a fundamental right means that it cannot be alienated, and therefore there is difficulty, from the perspective of the EU, in reconciling personal information, which is the key feature of data protection, as a commodity that can be traded or exchanged. On the other hand, the EU does recognise the importance and value of personal information in fostering economic growth, job creation and enhancing societal progress. Moreover, the free flow of personal information is critical to achieving these objectives. As a result, the aim of the GDPR is to achieve a balance between promoting the fundamental right to data protection and the free flow of information. In so doing, the EU data protection rules appear to legitimise rather than discourage the trade in personal information and therefore endorse the commodification of personal information. Data subjects have property-like rights over their personal information that allow them to safeguard dignity and autonomy as well as advance their economic interests.

UNIVERSITY of the
WESTERN CAPE

There is no doubt that the EU legislative framework governing the protection of personal information is at odds with preserving personal information as a fundamental right and encouraging data flows for economic reasons. The EU persists with the rhetoric that personal information is not a commodity and therefore cannot be economically exploited. Although this is not an issue in and of itself, building an economy around something that is seemingly not considered a commodity suggests otherwise. The GDPR offers a potentially a higher level of data protection compared to POPIA and the various US sectoral statutes. However, it appears unable of altering the notion that personal information is commodifiable. It is a fact that the trade in personal information is widespread, and therefore the argument that personal information cannot be commodified based on human rights concerns is no longer tenable.

Advances in technology and innovation have given rise to novel business models through which companies monetise personal information provided by data subjects in exchange for goods and services. The EU policymakers have acknowledged this fact and, as a response, have

https://uwcscholar.uwc.ac.za/home

implemented legislative instruments, such as the Digital Content Directive, to regulate such data practices. This appears to contradict the EU's established fundamental rights-based approach to treating personal information.

It ought to be recognised that personal information, when used as consideration or a medium of exchange, unlocks another dimension of something that is generally considered sacrosanct. In this context, the nature of personal information is transformed to primarily further the economic interests of the contractual parties and, in so doing, transcend the traditional boundary between what is considered inalienable and what is not. Personal information therefore becomes the subject of a contractual obligation.

The next chapter discusses the extent to which personal information may be characterised as property in the South African context.

UNIVERSITY of the
WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

CHAPTER SIX: EXPANDING ON THE CONCEPT OF CONSTITUTIONAL PROPERTY WITH SPECIFIC REFERENCE TO PERSONAL INFORMATION

6.1 INTRODUCTION 189

6.2 THE POSITION OF INFORMATION/ DATA AT COMMON LAW 190

6.3 INTERPRETING THE CONSTITUTIONAL PROPERTY CLAUSE 194

6.3.1 Textual interpretation 195

6.3.2 Purposive cum contextual interpretation 196

6.3.3 Teleological interpretation 198

6.3.4 Comparative aspects 199

6.3.5 Remarks 200

6.4 INFORMATION-BASED IMMATERIAL PROPERTY INTERESTS 201

6.5 PERSONAL INFORMATION AS CONSTITUTIONAL 'PROPERTY' 206

6.6 THE NEED FOR STATUTORY PROTECTION 210

6.7 CONCLUSION 211

https://uwcscholar.uwc.ac.za/home

6.1 INTRODUCTION

In chapters four and five, it was established that treating personal information as a commodity is a widespread phenomenon, regardless of whether the prevailing data protection legislative framework is founded on a model of marketplace discourse or fundamental rights. FIPs-inspired data protection legislation typically employs property-like rules to confer exclusion rights on individuals and allow for some form of transferability with respect to personal information. This further supports an argument that property rights in personal information are a reasonable proposition.

The US and EU have adopted the stance that personal information cannot be legally recognised as property. From a US perspective, the free flow of data that is so necessary for innovation would be adversely affected if personal information were, in any sense, to be propertised. In the EU context, personal information cannot be treated as an economic asset as this would undermine the individuals' dignity and fundamental rights to privacy and data protection. Moreover, the use of traditional property concepts, such as ownership and alienability, does not appear to be suitable when applied to personal information.

In this chapter, the question of whether personal information could be deemed property is explored from a South African perspective. This is novel in the South African context, as personal information is generally only discussed in relation to privacy and data protection.[1160] Van der Walt states that transformation, specifically with reference to property law post-1994, ought to steer our understanding of what property is.[1161] In chapter three, the transformative nature of the Constitution was highlighted and the role it is expected to play in fostering the right to privacy and, ultimately, the right to dignity.[1162] It is submitted that the Constitution is expected to play a similar role with respect to the right to property.

The chapter begins with a summary of the legal status of information or data under common law and the expressed objections to its treatment as property. Next, the common law will be analysed as to whether courts are able to develop it sufficiently to address the problems posed by the commodification of personal information. The principles of constitutional interpretation will then be discussed to see how these principles have been applied in the context of the constitutional property clause. An overview is then provided of traditional immaterial property

[1160] See 1.2 above.
[1161] Van der Walt A *Property and Constitution* (2012) 122.
[1162] See 3.6 above.

https://uwcscholar.uwc.ac.za/home

rights and certain unconventional information-based immaterial property interests that have been recognised as 'property' for constitutional purposes. The interpretation principles will then be applied to determine whether personal information could qualify as constitutional property. Finally, the dissertation touches on why statutory protection is required in this case to give effect to the constitutional right to property.

6.2 THE POSITION OF INFORMATION/ DATA AT COMMON LAW

Data is commonly described as the 'new oil' because of its value, when refined, in fuelling economic growth and creating new opportunities.[1163] This metaphor implies that the data ownership can lead to wealth creation.[1164] Zech opines that the notion of 'data property' is a contentious topic.[1165] According to Njotini, there has been a long-standing debate about whether information ought to be regarded as property.[1166] No courts have pronounced on whether or not real rights in information exists in South Africa.[1167]

Even though we can record information on a tangible object like paper, the information itself is intangible.[1168] Historically, information was not legally recognised as property. In Roman law, the Institutes of Justinian provide that, '… if Titius writes a poem, or a history, or a speech on your paper and parchment, the whole will be held to belong to you, and not to Titius'.[1169] In the Canadian case, *R v Stewart*,[1170] the court held: 'The "taking" of an intangible could only occur where such intangible is embodied in a tangible object… . However, that would not result in the taking of the intangible *per se*, but rather of the physical object evidencing it.'[1171] These legal authorities imply that for legal purposes, only the paper containing the information is

[1163] See 0 above. See also Strowel A 'Big data and data appropriation in the EU' in T Aplin (ed) *Research Handbook on Intellectual Property and Digital Technologies* (2020) 107.
[1164] Nolin J 'Data as oil, infrastructure or asset? Three metaphors of data as economic value' (2020) 18 *Journal of Information Communication and Ethics in Society* 28 34.
[1165] Zech H 'Information as property' (2015) 6 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* para 34.
[1166] Njotini M 'Evaluating the position of information or data in the law of property' (2015) 26 *Stellenbosch Law Review* 220 225.
[1167] Njotini M *E-Crimes and E-Authentication – Legal Perspective* (unpublished LLD thesis, University of South Africa, 2016) 67.
[1168] Nimmer R & Krauthaus P 'Information as a commodity: New imperatives of commercial law' (1992) 55 *Law and Contemporary Problems* 103 105.
[1169] Moyle J *The Institutes of Justinian:* 2.1.33 5 ed (1913) available at https://droitromain.univ–grenoble–alpes.fr/Anglica/just2_Moyle.htm#II (accessed 19 October 2022).
[1170] [1988] 1 SCR 963 (SCC).
[1171] [1988] 1 SCR 963 979g–h (SCC).

https://uwcscholar.uwc.ac.za/home

considered property. This suggests that for property rights to exist in an object, it must have a corporeal existence.

Courts have traditionally viewed the privatisation of information with scepticism. In *Waste-tech (Pty) Ltd v Wade Refuse (Pty) Ltd*,[1172] the court held that '… information or knowledge, of whatever value and however confidential, is not recognised as property either in South Africa or in the English law systems'.[1173] In the English case of *Boardman v Phipps (Boardman)*,[1174] Lord Upjohn stated that, '[i]n general, information is not property at all. It is normally open to all who have eyes to read and ears to hear'.[1175] The *Boardman* decision suggests that information cannot be considered property because it is easily accessible to all. One of the inherent characteristics of property is excludability.[1176]

However, even in those instances where confidentiality is maintained, there is substantial authority against recognising property rights in confidential information. The question of whether property rights exist in confidential information was considered in *Oxford v Moss (Moss)*.[1177] A student was charged with theft after dishonestly gaining access to confidential information for the purposes of memorising the information to cheat in an examination.[1178] It was contended that there was no intention by the student to physically deprive the university of the confidential information.[1179] The court determined that the confidential information did not fall within the definition of intangible property and was therefore not susceptible to theft.[1180]

A similar position was adopted by the South African courts in *Dun and Bradstreet (Pty) Ltd v SA Merchants Combined Credit Bureau (Cape) (Pty) Ltd.*[1181] In this case, the plaintiff, a credit bureau, compiled credit information that it distributed on a confidential basis to its subscribers. The defendant obtained copies of these credit records in an unauthorised manner and shared the information with its own subscribers. The plaintiff sought damages from the defendant, claiming, among other things, that the credit information constituted incorporeal property and

[1172] [1993] 3 All SA 542 (W).
[1173] [1993] 3 All SA 542 (W) 555.
[1174] (1967) 2 AC 46.
[1175] (1967) 2 AC 46 127.
[1176] See 4.10.2 above.
[1177] (1979) 68 Cr App R 183.
[1178] (1979) 68 Cr App R 183.
[1179] (1979) 68 Cr App R 183 184.
[1180] (1979) 68 Cr App R 183 184–85.
[1181] 1968 (1) SA 209 (C).

https://uwcscholar.uwc.ac.za/home

that the defendant had infringed its copyright.[1182] Corbett J (as he then was) rejected the plaintiff's argument that confidential information was property.[1183] The Canadian case, *R v Stewart*,[1184] likewise rejected the idea that confidential information constitutes property that can be the subject of theft.[1185] The courts' reasoning again illustrates the misplaced emphasis on physical existence.

Despite the historical preponderance of authority opposing the notion of property rights in information, there is growing recognition of the value of information and a receptiveness to considering the existence of proprietary interests in information. In *Fairstar Heavy Transport NV v Adkins*,[1186] the court remarked in dicta that it would be unwise to endorse a proposition that information could never be property.[1187] In *Regina (Veolia ES Nottinghamshire Ltd) v Nottinghamshire County Council*,[1188] the court held that '… confidential information is a well recognised species of property, protected by the common law and recognised in other relevant statutes… . Commercial confidential information may well constitute the life blood of an enterprise'.[1189] Likewise, in *Harchris Heat Treatment (Pty) Ltd v Iscor*,[1190] the court treated confidential information as a form of property.[1191]

It is recognised that certain types of intangible, information-based interests, such as confidential information, trade secrets and commercial information, by their very nature, possess certain proprietary features, namely economic value, usefulness and excludability.[1192] The holder of such information can exploit the information for commercial gain or use it to obtain a competitive advantage because it is not known to others. The holder may be the person that developed the information or the person to whom it is transferred through an assignment

[1182] 1968 (1) SA 209 (C) 210C–F.
[1183] 1968 (1) SA 209 (C) 215H.
[1184] [1988] 1 SCR 963 (SCC).
[1185] [1988] 1 SCR 963 979d (SCC).
[1186] (2013) EWCA Civ 886.
[1187] (2013) EWCA Civ 886 para 48.
[1188] (2010) EWCA Civ 1214.
[1189] (2010) EWCA Civ 1214 para 111.
[1190] 1983 (1) SA 548 (T).
[1191] 1983 (1) SA 548 (T) 555E. In this case, confidential information was held to be a form of intellectual property.
[1192] Knobel J 'Wrongfulness of trade secret misappropriation; and trade secrets as objects of subjective rights' (2000) *Acta Juridica* 196 203; Neethling J 'Appropriation of competitor's business ideas: Acquisition and use of competitor's trade secrets or confidential information; misappropriation of competitor's performance' in Van Heerden H & Neethling J (eds) *Unlawful competition* 2 ed (2008) 136; Kellerman M *The Constitutional Property Clause and Immaterial Property Interests* (unpublished LLD thesis, University of Stellenbosch, 2011) 57–60.

https://uwcscholar.uwc.ac.za/home

or licensing arrangement. Therefore, certain scholars (such as Kellerman) have advocated for such interests to be protected as property under s 25 of the Constitution.[1193]

These decisions offer some authority on the interpretation and application of common law principles to recognise and protect various information-based interests. The question then arises as to whether the common law notion of property could be extended to include personal information. Establishing the common law's position is necessary before developing it.[1194] For something to qualify as property, it must:[1195] (1) be useful and valuable; (2) exist independently and not merely be a part of something else; (3) exist separately from the human body; and (4) be subject to human control. An object that satisfies these criteria is susceptible to ownership, which at common law confers on the owner the most complete powers over a thing to do with as he or she chooses within the confines of the law.[1196] This entails the unrestricted and exclusive control over an object.

Under common law, could 'personal information' qualify as property? Traditionally, personal information is viewed as a part of the human personality and therefore cannot be commodified.[1197] As such, personal information was not something that could be conceptualised in property terms. In other words, personal information could not be owned in the conventional sense. Moreover, as is the case with intangible interests in general, personal information is characterised by its non-rivalrous and non-excludable nature.[1198] Therefore, it is submitted that common law principles of property cannot be adapted to accommodate personal information.

The envisaged propertisation of personal information is a distinct yet interconnected matter to the protection of personal information. This is because the very same data practices that threaten the constitutional right to privacy may also implicate the constitutional right to property. As stated previously, private persons wield enormous power that can infringe the rights of others.[1199] Moreover, the use of big data analytics to identify consumer interests and

---

[1193] Kellerman M (2011) 57–60.

[1194] *Mighty Solutions t/a Orlando Service Station V Engen Petroleum Ltd And Another* 2016 (1) SA 621 (CC) para 39. See De Vos P & Freedman W (eds) *South African Constitutional Law in Context* (2014) 782 for an explanation of the term 'common law'.

[1195] Thaldar D et al 'The multidimensional legal nature of personal genomic sequence data: A South African perspective' (2022) *Frontiers in Genetics* 1 4.

[1196] Van der Walt A & Pienaar G *Introduction to the Law of Property* 7 ed (2016) 28; Thaldar D & Shozi B 'The legal status of human biological material used for research' (2021) 138 *SALJ* 881 883–4.

[1197] See 1.2 above.

[1198] See 4.10.2 above.

[1199] See 3.6.2 above. See the example of *Facebook-Cambridge Analytica* in 2.3.3 above.

https://uwcscholar.uwc.ac.za/home

influence decision-making to generate revenue facilitates the commodification of personal information.[1200] Therefore, there is a need to determine whether s 25 of the Constitution can be interpreted to encompass personal information as a form of property. These difficulties give birth to intricate challenges that necessitate legislative intervention.[1201] Therefore, the introduction of a property regime for personal information will require substantial legislative reforms rather than incremental changes to the common law.[1202] This aspect will be discussed below.[1203]

6.3 INTERPRETING THE CONSTITUTIONAL PROPERTY CLAUSE

Section 25 of the Constitution contains the property clause that provides for the protection of property as a fundamental right. When considering the range of interests that the term 'property' could encompass, it is important to examine the relevant principles governing constitutional interpretation.[1204] Interpretation of any document of every kind, including legislation, legal instruments and contracts, is one unitary exercise.[1205] In other words, interpretation is not a process that occurs in sequential steps. This means that the interpretation exercise is to be approached holistically; that is, the text, purpose and context are to be considered simultaneously with none predominating the other.[1206] Section 39(1) of the Constitution provides that:

'When interpreting the Bill of Rights, a court, tribunal or forum – (a) must promote the values that underlie an open and democratic society based on human dignity, equality and freedom; (b) must consider international law; and (c) may consider foreign law'.

[1200] See chapter two.

[1201] Burns Y & Burger-Smidt A *Protection of Personal Information: Law and Practice* 2 ed (2023) 13–4.

[1202] Neethling J 'Features of the Protection of Personal Information Bill, 2009 and the Law of Delict' (2012) 75 *THRHR* 241 245; *Mighty Solutions t/a Orlando Service Station V Engen Petroleum Ltd And Another* 2016 (1) SA 621 (CC) para 44.

[1203] See 6.6 below.

[1204] For principles of interpretation see generally *Cool Ideas 1186 CC v Hubbard* 2014 (4) SA 474 (CC) para 28; *Chisuse and Others v Director-General, Department of Home Affairs and Another* 2020 (6) SA 14 (CC) para 47.

[1205] *Natal Joint Municipal Pension Fund v Endumeni Municipality* 2012 (4) SA 593 (CC) paras 18–9.

[1206] *Chisuse and Others v Director-General, Department of Home Affairs and Another* 2020 (6) SA 14 (CC) para 52; *University of Johannesburg v Auckland Park Theological Seminary and Another* 2021 (6) SA 1 (CC) para 65.

https://uwcscholar.uwc.ac.za/home

This interpretation clause must be read with the supremacy clause which states that the Constitution is the supreme law of the country.[1207] Therefore, the Constitution must be interpreted and applied in the light of its normative framework, which is based on a set of fundamental values.[1208] The effect would be that the interpretation process already incorporates the fundamental values before it commences. Moosa states that interpreters of the Constitution must have a transformational mindset to uncover the values immanent in s 25 to promote its fullest protection.[1209] This will ensure that the concept of 'property' is shaped by the values underpinning the Constitution.

6.3.1 Textual interpretation

Interpretation begins with the text itself. Consideration must be given to the ordinary grammatical meaning of the words, rules of syntax and other structural components of the text.[1210] Interpreters must respect the language employed to articulate the rights in s 25(1) of the Constitution.[1211] However, this does not imply a mechanical adherence to a legalistic interpretation.[1212] Instead, a generous interpretation must be preferred to afford beneficiaries the fullest possible protection of their constitutional guarantees.[1213] Therefore, the term 'property' must not be interpreted restrictively, except to the extent permitted by the limitation clause contained in s 36 of the Constitution.[1214]

Section 25(1) expressly refers to property and not ownership of property.[1215] Moosa argues, correctly in my view, that the scope of 'property' ought to extend beyond things that are subject to real rights of ownership or limited real rights to include other things such as personal rights.[1216] Applying a generous interpretation expands the ambit of 'property' beyond the

[1207] Section 2, Constitution.
[1208] *S v Zuma and Others* 1995 (2) SA 642 (CC) para 14; *Pharmaceutical Manufacturers Association of SA & Another: In re Ex Parte President of the Republic of South Africa and Others* 2000 (2) SA 674 (CC) para 44.
[1209] Moosa F 'Understanding the "Spirit, Purport and Objects" of South Africa's Bill of Rights' (2018) 4 *Journal of Forensic, Legal & Investigative Sciences* 1 2.
[1210] *Natal Joint Municipal Pension Fund v Endumeni Municipality* 2012 (4) SA 593 (CC) para 18.
[1211] Moosa F 'Is Cryptocurrency "Property" for Tax Administration Purposes?' (2021) 33 *SAMLJ* 364 373; *S v Zuma and Others* 1995 (2) SA 642 (CC) para 17.
[1212] *Department of Land Affairs and Others v Goedgelegen Tropical Fruits* 2007 (6) SA 199 (CC) para 53; *Klaase and Another v Van Der Merwe N.O and Others* 2016 (6) SA 131 (CC) para 51.
[1213] Moosa F (2021) 373; *Department of Land Affairs and Others v Goedgelegen Tropical Fruits* 2007 (6) SA 199 (CC) para 53.
[1214] Moosa F (2021) 373.
[1215] See 4.9.3 above.
[1216] Moosa F (2021) 377.

https://uwcscholar.uwc.ac.za/home

common law meaning of ownership to include other entitlements, such as the bundle of rights that make up ownership.[1217] In this way, property is described as a bundle of rights in relation to others that is separate from the 'thing' that is owned. Therefore, the focal point is no longer the actual 'thing', which allows for the possibility of conceiving new rights and interests. It is submitted that a concept of property as a bundle of rights aligns with s 25(4)(b) of the Constitution, which reads: 'property is not limited to land'. This bundle of rights concept is demonstrated in the context of data protection, in which data protection legislation employs property-like entitlements to regulate the processing of personal information.[1218]

6.3.2 Purposive cum contextual interpretation

Purposive interpretation is the interpretation of a provision that gives effect to a meaning that best advances the core values that underpin an open and democratic society based on human dignity, equality and freedom.[1219] The Constitution requires the use of a purposive and contextual approach to clarify the scope and intended effect of a provision.[1220] Purposivism means that the language used in the provision must be considered in relation to contextual considerations and the purpose to which it is directed.[1221]

According to South African constitutional property jurisprudence, s 25 of the Constitution ought to be interpreted in a manner that promotes transformation, reform and development by redressing past injustices.[1222] Such an interpretation ensures that the Constitution's protective role does not compromise its reformative aims.[1223] This means that the Constitution is

[1217] Moosa F (2021) 377.

[1218] See 5.4.1 for a discussion of the GDPR. It is submitted that the bundle of rights concept would be equally applicable to other data protection legislation such as POPIA, the CCPA, and most FIP-based regulations, irrespective of whether they are framed in human rights terms or not.

[1219] Currie I & De Waal J *The Bill of Rights Handbook* 6 ed (2013) 136; Moosa F (2018) 2.

[1220] *Bato Star Fishing (Pty) Ltd v Minister of Environmental Affairs and Others* 2004 (4) SA 490 (CC) paras 89–91; *Bertie Van Zyl (Pty) Ltd and Another v Minister for Safety and Security and Others* 2010 (2) SA 181 (CC) para 21.

[1221] *Natal Joint Municipal Pension Fund v Endumeni Municipality* 2012 (4) SA 593 (CC) paras 18–20.

[1222] *FNB* 2002 (4) SA 768 (CC) para 49; *Mkontwana v Nelson Mandela Metropolitan Municipality; Bissett v Buffalo City Municipality; Transfer Rights Action Campaign v MEC, Local Government and Housing, Gauteng* 2005 (1) SA 530 (CC) para 81; *Mphela and Others v Haakdoornbult Boerdery CC and Others* 2008 (4) SA 488 (CC) paras 28–9.

[1223] *Agri South Africa v Minister for Minerals and Energy* 2013 (4) SA 1 (CC) paras 60–5; Marais E (2016) 576. Mostert H 'Engaged citizenship and the enabling state as factors determining the interference parameter of property: A comparison of German and South African law' (2010) 127 *SALJ* 238 239 points out that the constitutional property clause is characterised by an inherent tension between the protective and reformative aspects. For a brief overview of the dichotomy between the protective and reformative aspects, see Currie I and De Waal J *The Bill of Rights Handbook* (2013) 531–32.

https://uwcscholar.uwc.ac.za/home

backward- and forward-looking.[1224] According to Moosa, the spirit of transformation must inform the meaning of property in its context to advance the realisation of the Constitution's goals.[1225] Therefore, the context, whether historical, socio-economic, or constitutional, as well as the merits of each case are important factors when interpreting s 25.[1226] Purposive interpretation entails, first, identifying the purpose of a right in the Bill of Rights and, secondly, objectively determining which value it protects and the scope of the right.[1227]

In *Shoprite Checkers (Pty) Ltd v MEC for Economic Development, Environmental Affairs and Tourism, Eastern Cape (Shoprite)*,[1228] Froneman J states: 'The question of property is fiercely contested in South African society. There is, as yet, little common ground on how we conceive of property under s 25 of the Constitution, why we should do so, and what purpose the protection of property should serve.'[1229] The CC, in *First National Bank of SA Ltd t/a Wesbank v Commissioner; South African Revenue Service; First National Bank of SA Ltd t/a Wesbank v Minister of Finance (FNB)*,[1230] considered the purpose of s 25 as a whole and identified two goals, namely property rights serving the public interest, including but not limited to land reform and protecting private property rights.[1231]

UNIVERSITY of the
WESTERN CAPE

The CC indicated in *FNB* that the subsections contained in s 25 of the Constitution could not be interpreted in isolation but had to be considered in the context of the other provisions of s 25, their historical context and the context of the Constitution as a whole.[1232] In this regard, the CC held that ss 25(4)–(9) underscore the need to redress past injustices based on racial discrimination, which resulted in the grossly unequal distribution of land in South Africa.[1233] Many people were unjustly deprived of their property rights, leading to detrimental social and economic consequences.[1234] The CC also pointed out that, while these provisions were not

[1224] De Vos P & Freedman W (2014) 28.
[1225] Moosa F (2021) 375.
[1226] Van der Walt A 'Striving for the better interpretation - A critical reflection on the Constitutional Court's Harksen and FNB Decisions on the property clause' (2004) 121 *SALJ* 854 866.
[1227] Currie I & De Waal J (2013) 137; *S v Zuma and Others* 1995 (2) SA 642 (CC) para 15.
[1228] *Shoprite* 2015 (6) SA 125 (CC).
[1229] *Shoprite* 2015 (6) SA 125 (CC) para 4.
[1230] *FNB* 2002 (4) SA 768 (CC).
[1231] *FNB* 2002 (4) SA 768 para 50. The property clause's protective function is found in the negatively framed right to property in ss 25(1)–(3). The property clause's reform function is found in ss 25(5)–(9).
[1232] *FNB* 2002 (4) SA 768 (CC) para 49.
[1233] *FNB* 2002 (4) SA 768 (CC) para 49.
[1234] Moosa F (2021) 376.

https://uwcscholar.uwc.ac.za/home

necessarily relevant to the *FNB* case, they ought to be kept in mind whenever s 25 is interpreted.[1235]

The purposive approach of s 25 highlights the tension between the opposing objectives of land redress and the protection of private property against arbitrary deprivation. In this regard, s 25 must be seen as seeking to strike a proportionate balance between safeguarding private property rights and serving the public interest in the sphere of land reform.[1236] These interests serve as a background for interpreting the property clause and implies that consideration of the context is important in interpreting s 25. Therefore, it becomes almost impossible to establish a single, abstract interpretation of the property clause, as it is always dependent on the context, the characteristics and the requirements of each case.[1237] In this regard, the CC has broadened the concept of property for the purposes of s 25 of the Constitution.[1238]

6.3.3 Teleological interpretation

A teleological interpretation of s 25 requires a consideration of the context of the Bill of Rights as well as the fundamental values underpinning the Constitution.[1239] Therefore, the purpose of s 25, as identified, ought to be informed by the fundamental values of the Constitution. These values are guiding principles and contribute to the realisation of the Constitution's aims, ethos and culture.[1240]

In *Shoprite*, Froneman J writing for the majority,[1241] employed a teleological approach, in terms of which he found it necessary to determine whether the purpose behind the constitutional protection of property was reconcilable with the values underpinning the Constitution.[1242] According to Froneman J, these values require a conception of property that allows for individual self-fulfilment on the one hand and recognising that the holding of

[1235] *FNB* 2002 (4) SA 768 (CC) para 49.
[1236] Van der Walt A (2004) 866.
[1237] Van der Walt A (2004) 866.
[1238] See 6.4 below.
[1239] Mupangavanhu B 'Impact of the Constitution's Normative Framework on the Interpretation of Provisions of the Companies Act 71 of 2008' (2019) 22 *PELJ* 1 6–7; Donald M 'Unlocking the Potential of Wellbeing in the Environmental Right: A Teleological Interpretation' (2020) 31 *Stellenbosch Law Review* 55 63.
[1240] Moosa F (2021) 372.
[1241] Froneman J together with Cameron J, Jappie AJ and Nkabinde J and Madlanga J together with Tshiqi J accepted that a liquor licence is property. However, Madlanga J disagreed with the approach followed by Froneman J.
[1242] Marais E (2016) 578.

https://uwcscholar.uwc.ac.za/home

property must not harm the public good on the other.[1243] Moreover, if the holding of property advances other fundamental rights, the level of protection afforded to that property will be greater.[1244]

Froneman J held that a liquor licence ought to be recognised as constitutional property as it promotes self-fulfilment, not to maximise wealth creation or satisfy individual preferences, but to secure living a life of dignity and in recognition of the dignity of others.[1245] Therefore, the interpretation contended for here means that a constitutional concept of privacy cannot be restricted to a private-law notion of property, as this would impede the Constitution from meeting the needs of a developing society, thus preventing it from fulfilling its transformation objectives.[1246]

6.3.4 Comparative aspects

Section 39(1) also provides that a court, tribunal or forum must consider international law when interpreting the Bill of Rights and may consider foreign law.[1247] In this regard, international law must be considered by a court, but it is not mandatory to apply it. In this dissertation, a comparative law methodology is followed to analyse the treatment of personal information in other jurisdictions, specifically the US and the EU.

The analysis reveals that the treatment of personal information as a commodity is a widespread phenomenon. Chapter four demonstrated how the US protects the individual as a consumer in the personal data marketplace. As such, the individual is free to trade his or her personal information for benefits.[1248] However, due the prioritisation of liberty interests, it is not likely that the US will recognise property rights in personal information as labelling personal information as property may impede the flow of data. In chapter five, EU perspective reveals that personal information cannot be seen as an economic asset, since doing so would compromise the dignity and fundamental rights of individuals to privacy and data protection.

[1243] *Shoprite* 2015 (6) SA 125 (CC) para 50.
[1244] *Shoprite* 2015 (6) SA 125 (CC) para 50.
[1245] *Shoprite* 2015 (6) SA 125 (CC) para 50.
[1246] Moosa F (2021) 380; *Shoprite* 2015 (6) SA 125 (CC) para 46.
[1247] See ss 39(1)(b) and 39(1)(c) of the Constitution.
[1248] See 4.1 and 4.2 above.

https://uwcscholar.uwc.ac.za/home

However, the recognition of personal information as a commodity is implicit in the adoption of various legislative instruments like the CCPA in the US and the Digital Content Directive in the EU.[1249] These instruments recognise that personal information can have economic value. In this regard, a judgment by an Italian regional administrative court held that viewing personal data only from a data protection perspective 'represents a simplistic and partial view of their inherent potential'.[1250] The court held further that personal data could constitute an economic asset 'capable of assuming the function of consideration (counter-performance) of a contract in the technical sense'.[1251]

Moreover, data protection legislation, such as the GDPR and CCPA, employs property-like entitlements to regulate the processing of personal information.[1252] Therefore, when interpreting the constitutional property clause, it is important to consider developments and practices in other jurisdictions. This is because South Africa is also susceptible to the data practices that give rise to the commercialisation of personal information.

6.3.5 Remarks

UNIVERSITY of the
WESTERN CAPE

An interpretation of a provision contained in the Bill of Rights ought to be consistent with the language used in the text, its purpose, and the context of the provision itself, as well as with the Constitution. The flexibility of the constitutional text creates room to attribute meaning to the fundamental rights, depending on the context. In so doing, a deliberate decision is made to apply a transparent and democratic set of values to build and sustain a society that is empowered and advances the rule of law, economic participation, and respect for human rights and freedoms. In other words, these values must be infused into the interpretive process and inform the decision to recognise (or not recognise) a particular thing as property. This allows for the property clause to be interpreted expansively so that it advances protection for the values underpinning the Constitution. These principles of interpretation will be applied in the case of

[1249] See 4.7.4 and 5.5 for a discussion on the CCPA and the Digital Content Directive respectively.

[1250] Propato M & Zannoni L 'The Debate over Data Monetization – an EU (and Italian) Perspective' 13 June 2022 available at *https://www.dentons.com/en/insights/articles/2022/june/13/the-debate-over-data-monetization-an-eu-and-italian-perspective* (accessed 24 May 2024). The Italian version of the judgment can be accessed at *https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=tar_rm&nrg=201815288&nomeFile=202000261_01.html&subDir=Provvedimenti*.

[1251] Propato M & Zannoni L 'The Debate over Data Monetization – an EU (and Italian) Perspective' 13 June 2022.

[1252] See 5.3.3 for a discussion on the GDPR.

https://uwcscholar.uwc.ac.za/home

personal information below.[1253] However, the next section will first explore the various intangible interests that the CC has recognised as constitutional property.

6.4 INFORMATION-BASED IMMATERIAL PROPERTY INTERESTS

Property and trade are interconnected.[1254] Confidential information, trade secrets, commercial information and intellectual property are generally regarded by businesses as important assets.[1255] These assets allow the owner or holder to have a competitive advantage in the marketplace. Moreover, they represent knowledge, which propels data-driven innovation and development.[1256] The loss or destruction of such assets due to disclosure or lost intellectual property protection would inevitably lead to a loss in profits for the owner or holder. The recognition of unconventional, intangible property interests underscores the significance of their function in the modern economy.[1257] Consequently, the CC has recognised a wide range of traditional and unconventional, intangible property interests as property under s 25 of the Constitution.

UNIVERSITY of the
WESTERN CAPE

While s 25 of the Constitution guarantees the protection of property as a fundamental right, the Constitution does not define the term 'property'.[1258] The CC in *FNB* held that the ownership of corporeal property and land is fundamental to the constitutional concept of property;[1259] however, this does not imply that property will only fall into these categories.[1260] In *FNB*, the CC found it 'practically impossible to furnish – and judicially unwise to attempt – a comprehensive definition of property for the purposes of s 25'.[1261] Subsequently, in *Law Society of South Africa v Minister of Transport*,[1262] the CC held that the definition of

[1253] See 6.5 below.
[1254] Moosa F (2021) 379.
[1255] See 6.2 above.
[1256] Chidede T 'The role of intellectual property rights' protection in advancing development in South Africa' (2022) 26 *Law, Democracy & Development* 168 172 interprets 'development' broadly to encompass the maximisation of wealth and income as well as improving the lives and freedoms of individuals.
[1257] Marais E (2016) 580; *National Credit Regulator v Opperman* 2013 (2) SA 1 (CC) para 63.
[1258] *National Credit Regulator v Opperman* 2013 (2) SA 1 (CC) para 60.
[1259] *FNB* 2002 (4) SA 768 (CC) para 51.
[1260] See also 25(4)(b) which provides that property is not limited to land.
[1261] *FNB* 2002 (4) SA 768 (CC) para 51.
[1262] 2011 (1) SA 400 (CC).

https://uwcscholar.uwc.ac.za/home

constitutional property should not be too wide to make legislative regulation impracticable nor so narrow to render the protection of property worthless.[1263]

As regards its subject matter, s 25(1) appears to be directed or aimed at three things. First, the property itself, or those things with respect to which legal relations between individuals exist; secondly, the set of legal rules that govern relationships between individuals and property; and thirdly, the relationships or interests having an exchange value.[1264] For the purposes of this dissertation, this last category is especially relevant in light of personal information being commoditised. Hence, emphasis is laid thereon in the ensuing discussion.

The CC has used an incremental approach to determine whether a particular interest constitutes property for constitutional purposes under s 25 by having regard to the facts of each case.[1265] As a result, the CC has, over the years, recognised various forms of intangibles as 'property' for constitutional purposes. The CC often bases this recognition on the assumption that the various interests are property for constitutional purposes without conducting any analysis.

The following is a synopsis of cases involving intangible and/or unconventional property interests which were judicially recognised as constituting "property" for constitutional purposes:

- In *Laugh It Off Promotions CC v SAB International (Finances) BV*,[1266] the CC accepted that trademarks,[1267] and therefore other forms of intangible property already recognised as property under private law, enjoyed protection under s 25.[1268]

- In *Phumelela Gaming and Leisure Ltd v Grundlingh (Phumelela),*[1269] the CC accepted, without conducting any analysis, that goodwill was property for the purposes of s 25.[1270] *Phumelela* is significant in the context of this dissertation as goodwill is an

[1263] 2011 (1) SA 400 (CC) para 83.
[1264] Currie I & De Waal J (2013) 535.
[1265] *FNB* 2002 (4) SA 768 (CC) para 51; Currie I & De Waal J (2013) 535.
[1266] 2006 (6) SA 144 (CC).
[1267] 2006 (6) SA 144 (CC) para 17.
[1268] Du Bois M 'Intellectual Property as a Constitutional Property Right: The South African Approach' (2012) 24 *SAMLJ* 177 179–80. See also *Ex Parte Chairperson of the Constitutional Assembly: In Re Certification of the Constitution of the Republic of South Africa, 1996* 1996 (4) SA 744 (CC) para75 in which the CC held that the meaning of 'property' as contemplated in the constitutional property clause was wide enough to include intellectual property and, therefore, there was no requirement for it to be dealt with separately under the Bill of Rights.
[1269] 2007 (6) SA 350 (CC).
[1270] 2007 (6) SA 350 (CC) paras 32–42.

https://uwcscholar.uwc.ac.za/home

intangible interest that may also be described as an unconventional property interest since it is not necessarily recognised as property in private law but does have commercial value.[1271]

- It was argued by the applicants in *Law Society of South Africa v Minister for Transport (Law Society*),[1272] that claims against the Road Accident Fund for medical costs, the loss of earning capacity, and loss of support constitute a bundle of rights or rights with monetary value and therefore fall within the meaning of property for the purposes of s 25.[1273] The applicants relied on the *Phumelela* case to compare what goodwill is to a juristic person to what earning capacity is to a natural person.[1274] The CC decided not to debate whether claims for loss of earnings or support were property and simply accepted them as such.[1275] As with *Phumelela*, *Law Society* expanded the definition of property to include an interest that is intangible and which is not recognised or protected as property in private law.

- In *National Credit Regulator v Opperman (Opperman),*[1276] the CC held that the right to restitution of money paid, based on an unjustified enrichment claim, was property for the purposes of s 25.[1277] The CC reasoned that the claim had monetary value, could be transferred or disposed of, and therefore constituted an asset.[1278] These qualities serve as the standards by which a thing or an interest qualifies as property under private law. Again, the CC merely confirmed that an enrichment claim was property on the basis that it was a common cause between the parties,[1279] and to do so was 'logical and reasonable' under the circumstances.[1280] Significantly, the *Opperman* case does confirm the importance of intangibles in the context of a modern economy by extending protection to personal rights.

[1271] Kellerman M (2011) 17.
[1272] 2011 (1) SA 400 (CC).
[1273] 2011 (1) SA 400 (CC) para 81.
[1274] 2011 (1) SA 400 (CC) para 81.
[1275] 2011 (1 SA 400 (CC) paras 83–4.
[1276] 2013 (2) SA 1 (CC).
[1277] 2013 (2) SA 1 (CC) para 64.
[1278] 2013 (2) SA 1 (CC) para 58.
[1279] 2013 (2) SA 1 (CC) para 59.
[1280] 2013 (2) SA 1 (CC) para 63.

https://uwcscholar.uwc.ac.za/home

- In *Shoprite*,[1281] the CC had to decide, among other things, whether a commercial trading licence that permits the sale of wine constitutes property under s 25 of the Constitution.[1282] Froneman J recognises the need for a constitutional notion of property that extends beyond the private concept of property to allow for the later inclusion of other potential constitutional entitlements that may deserve protection and to ensure that s 25 does not become an obstacle to transformation.[1283] Froneman J, writing for the majority, held that a trading licence was indeed property by adopting a values-based approach based on the fundamental values of dignity, equality and freedom to conclude that a wine licence is constitutional property.[1284] On the other hand, Madlanga J, in his dissenting opinion, agrees that the licence ought to be recognised as property but this is because it possesses the attributes of the private law concept of property.[1285] Despite Froneman J and Madlanga J adopting different approaches to finding that a wine license is property for the purposes of s 25, both rely on a private law understanding of property to decide the property question in addition to the constitutional values.[1286] The *Shoprite* case is significant because the court conducted an analysis to determine the property question rather than making assumptions as in previous CC decisions.

These decisions clearly demonstrate that the constitutional concept of property will include a broader range of interests than the private law notion of property. In this regard, Ackermann J stated in *FNB* that when interpreting s 25, it is necessary:[1287]

> '… to move away from a static, typically private law conceptualist view of the Constitution as a guarantee of the status quo to a dynamic, typically public law view of the Constitution as an instrument for social change and transformation under the auspices [and I would add "and control"] of entrenched constitutional values'.

[1281] See also 6.3.3 above.

[1282] *Shoprite* 2015 (6) SA 125 (CC) para 1. The other questions facing the CC were whether termination of such a license amounts to deprivation of property and, if so, whether such deprivation met the non-arbitrariness requirement in s 25. However, the deprivation aspect is beyond the scope of this dissertation.

[1283] *Shoprite* 2015 (6) SA 125 (CC) para 46.

[1284] *Shoprite* 2015 (6) SA 125 (CC) paras 46, 70.

[1285] *Shoprite* 2015 (6) SA 125 (CC) paras 72, 143.

[1286] Sono N 'Re-Examining the Constitutional Court's Approach to the Property Question Since First National Bank of SA Ltd T/A Wesbank v Commissioner, South African Revenue Service; First National Bank of SA Ltd T/A Wesbank v Minister of Finance 2002 4 SA 768 (CC)' (2022) 25 *PELJ* 1 13–5.

[1287] *FNB* 2002 (4) SA 768 (CC) para 52.

https://uwcscholar.uwc.ac.za/home

The incremental approach adopted by the CC in developing the constitutional conception of property suggests that unconventional immaterial property interests not recognised hitherto could enjoy protection under s 25 of the Constitution, which is particularly relevant in the context of this dissertation. The CC has acknowledged the need for a constitutional concept of property that goes beyond a private law understanding of property to allow for the later inclusion of other potential constitutional entitlements that may deserve protection and to ensure that s 25 does not become an impediment to transformation.[1288]

It is possible to discern specific core characteristics among the information-based interests recognised by South African courts. First, is the intangible nature of the property interests concerned. For instance, copyright protects intellectual works that take on a physical form, enabling the intellectual creation to be distinguished from the tangible object it appears in.[1289] The alienation of the tangible object may not necessarily affect the intellectual creation.[1290] While many of these interests may be reduced to a tangible form, they generally do not need to occupy a physical space. In other words, these rights or interests cannot be physically touched.

Secondly, the property interests recognised have an inherent or accrued economic value for the holder of that interest and are capable of being useful, commercially or otherwise. It is clear from the CC property jurisprudence above that economic value is often quantified in monetary terms or enables the owner or holder to engage in business or trade.[1291] This is equally applicable to other interests, such as confidential information, trade secrets and commercial information.

Thirdly, the property rights recognised are also characterised by scarcity and excludability. In the case of confidential information, commercial information and trade secrets, maintaining secrecy or confidentiality allows such resources to be made scarce and excludable so that they are accessible only to authorised persons.[1292] In other instances, legislation is required to create

[1288] *Shoprite* 2015 (6) SA 125 (CC) para 46.
[1289] Dean O *The Application of the Copyright Act, 1978, to Works Made Prior to 1979* (unpublished LLD thesis, University of Stellenbosch, 1988) 3.
[1290] Dean O (1988) 3.
[1291] See 6.3 above.
[1292] See 6.2 above.

https://uwcscholar.uwc.ac.za/home

excludability, such as for intellectual property rights like copyright, so that only authorised persons can use that resource.[1293]

Fourthly, alienability or separability is considered an inherent feature of property. It was argued that full alienability is not an essential requirement for property.[1294] Therefore, limited alienability will suffice to meet the criteria for property. Limited alienability is often encountered in the licensing of intellectual property rights, in which a licensor grants a licensee the right to use or exploit such property without transferring ownership of the intellectual property to the licensee.

These characteristics are generally associated with a private law notion of property.[1295] However, the concept of property cannot be confined to its private law understanding. In this regard, Froneman J states that the constitutional concept of property must be rooted in the Constitution and cannot be dictated by pre-constitutional concepts of what property is, as this may exclude interests that deserve constitutional protection.[1296] Therefore, the constitutional concept of property will be wider than its private law counterpart to ensure that s 25 does not become an obstacle to transformation.[1297] According to Froneman J, the fundamental values of dignity, equality and freedom ought to inform the content of the constitutional right to property.[1298] The next section will delve into whether personal information may be protected as constitutional property.

6.5 PERSONAL INFORMATION AS CONSTITUTIONAL 'PROPERTY'

Established principles of constitutional interpretation ought to serve as the foundation for the interpretation of constitutional 'property'. If the Constitution is to remain relevant in the lives of ordinary South Africans, then it must be interpreted transformatively to keep pace with

[1293] Karjiker S *Open-Source Software and the Rationale for Copyright Protection of Computer Programs* (unpublished LLD thesis, University of Stellenbosch, 2013) 12 states that in the absence of statutory regulation, copyright and other forms of intellectual property are unable to satisfy the proprietary criteria of excludability and separability because of its intangible nature.

[1294] See 4.10.1 above.

[1295] Muller G et al *Silberberg and Schoeman's The Law of Property* 6 ed (2019) 18-26.

[1296] *Shoprite* 2015 (6) SA 125 (CC) para 46.

[1297] *Shoprite* 2015 (6) SA 125 (CC) para 46.

[1298] *Shoprite* 2015 (6) SA 125 (CC) paras 44, 46.

https://uwcscholar.uwc.ac.za/home

changing times and societal needs. This section will apply the principles of interpretation outlined above that integrate the purpose, context and underlying values of the Constitution.[1299]

Although s 25 of the Constitution entrenches the right to property, the text does not expressly refer to any type of property apart from land.[1300] However, s 25(4)(b) further provides that the notion of property is not limited to land. It is reasonable to presume that the drafters of the Bill of Rights intended to allow room for the judicial interpretation of the notion of 'property' and left the responsibility to the courts to determine what can be considered protectable property. Consequently, this makes the recognition of economically significant intangible interests, such as personal information, possible. Moreover, it is submitted that the drafters did not wish to be prescriptive as to what is or is not 'property', thereby allowing for courts to consider the development of the common law in a manner that promotes the spirit, purport and objects of the Bill of Rights as expressly catered for in s 39(2). This notwithstanding, it was concluded that the courts are unlikely to develop the common law to deal with personal information as a form of property.[1301]

The purpose of the constitutional property clause was delineated above and ought to be kept in mind whenever the property clause is interpreted.[1302] This would be the case even when the property interests involved are more commercial in nature and far removed from transformation issues like land reform.[1303] In other words, this approach would need to be followed when considering the possibility of protecting personal information as constitutional property.

In the context of the data-driven economy, it is evident that personal information has been commoditised.[1304] Data-driven innovation gives rise to new business models that are dependent on the processing of personal data.[1305] Individuals can acquire products and services by exchanging personal information, while businesses offering such products and services are able to monetise the personal information. Recognising the ensuing commodification of personal information is crucial for the law to respond appropriately, despite the unavoidable privacy risks. This commodification of personal information by the private sector and its use as a

[1299] See 6.3 above.
[1300] See s 25(4)(b) of the Constitution.
[1301] See 6.2 above.
[1302] See 6.3.2 above.
[1303] Van der Walt A (2004) 865; *FNB* 2002 (4) SA 768 (CC) para 49.
[1304] See chapters four and five above.
[1305] See 2.2.2 above.

https://uwcscholar.uwc.ac.za/home

medium of exchange suggest that it possesses certain property traits. These traits include alienability and excludability.[1306] Moreover, the fact that personal information is tradeable or can be monetised implies that it has economic value. Therefore, the recognition of private law property characteristics ought to be a factor in conceptualising new interests as constitutional property.[1307] While private law characteristics provide grounds for potentially recognising an interest as constitutional property, they should not be the determining factor.

Historically, the constitutional rights to privacy and property share a common heritage that influenced their transformative purpose.[1308] Under the apartheid regime, racial discrimination resulted in many non-white individuals being unlawfully dispossessed of their land and excluded from property ownership.[1309] The same apartheid regime also targeted those same race groups and routinely violated their privacy through unlawful searches.[1310] The actions of the apartheid government used the law as a blunt instrument to institutionalise unjust discrimination that demeaned and stripped individuals of their dignity.[1311] Consequently, both the rights to privacy and property attempt to provide a mechanism to address past wrongs and reaffirm practices that are consistent with the fundamental values underpinning the Constitution.

UNIVERSITY of the
WESTERN CAPE

In chapter three, it was established that the right to privacy fosters dignity.[1312] Since data protection is an aspect of privacy, it follows that they would share the same objective. To this end, the principles for the lawful processing of personal information contained in POPIA aim to, among other things, promote the data subject's dignity and autonomy.[1313] This is so because personal information plays a constitutive role with respect to personality. Therefore, there is an intrinsic link between personal information and dignity. However, the commodification of personal information undermines the protection provided to data subjects under privacy and

[1306] See 4.10.1 and 4.10.2 above.
[1307] *Opperman* 2013 (2) SA 1 (CC) para 58; *Shoprite* 2015 (6) SA 125 (CC) paras 67–8.
[1308] Moosa F (2021) 375–76.
[1309] See 6.3.2 above.
[1310] See 3.2.1 above.
[1311] Bilchitz D 'Privacy, Surveillance and the Duties of Corporations' (2016) 1 *TSAR* 45 49–50; Moosa F (2021) 376.
[1312] See 3.4 above.
[1313] See 3.3.3 above.

https://uwcscholar.uwc.ac.za/home

data protection legislation such as POPIA.[1314] It is submitted that commodification transforms personal information from something associated with personhood into a type of property.[1315]

In *Shoprite*, dignity was identified as an important value in determining whether something constituted property or not. Froneman J stated that determining whether an interest could be protected as constitutional property requires a conception of property that fosters individual self-fulfilment in order to lead a dignified life while respecting the dignity of others.[1316] In light of pervasive commodification, it is argued that individuals ought to be entitled to exercise autonomy and control over their personal information, which promotes personal development and allows them to lead dignified lives. The uniqueness of personal information as a potential property interest lies in its inherent link to dignity, regardless of its processing method, whether for commercial or non-commercial purposes. Therefore, it is submitted that personal information ought to qualify as constitutional property because it promotes dignity and autonomy.

To reject the notion that personal information may constitute constitutional property under certain circumstances means that the Constitution would have failed to fulfil its transformative potential, as it is no longer possible to ignore the widespread commoditisation of personal information. This would be akin to denying individuals their right to live with dignity, as was the case under apartheid. The only difference would be that it is not the state oppressing the masses but private sector actors.

Moreover, the fact that an interest does not sit comfortably with private law notions of property does not mean that it cannot be recognised as property under s 25 of the Constitution.[1317] The *Discovery v Liberty* (*Discovery*)[1318] case appears to expand unconventional property interests to include personal information as it exhibits these property attributes, which calls for a reconsideration of personal information as a potential commodity. Although *Discovery* does not deal with s 25 of the Constitution, it does provide a useful indication of how the law is developing with respect to the commodification of personal information.

[1314] POPIA does not conceive of personal information as a commodity and it may not offer adequate protection in such circumstances. See 3.5 above.
[1315] See 5.6 above.
[1316] *Shoprite* 2015 (6) SA 125 (CC) para 61.
[1317] *Opperman* 2013 (2) SA 1 (CC) paras 41, 59.
[1318] 2020 (4) SA 160 (GJ).

https://uwcscholar.uwc.ac.za/home

Discovery provides new authority pertaining to proprietary rights in personal information. Although the matter related primarily to a dispute concerning trademark infringement and unlawful competition, the judgement touches on the issue of data ownership. First, the court held that '… it is common cause that a Vitality member's Vitality status … is the members' personal information, and they are free to make it public'.[1319] It is therefore plausible to argue that Vitality information constitutes personal information as contemplated in POPIA and, as such, ought to enjoy protection under POPIA.

Secondly, the court provides that the owner of the personal information, in the absence of lawful restrictions, is entitled to share such information with a third party.[1320] This suggests that personal information belongs to the person to whom it relates, namely the data subject, and that such personal information may be treated as property by the data subject, which gives such a person the right to monetise their personal information.

While the court in *Discovery* did not investigate whether the personal information identified by it constitutes property, the decision *in casu* is significant because it: (i) allocates ownership of a resource; (ii) the court recognises the economic value of personal information; and (iii) the court recognises that personal information can be exchanged for something, criteria generally associated with the private law notion of property. Therefore, the court in *Discovery* envisages personal information as something that the owner of the information can commoditise and that another party can purchase.[1321]

UNIVERSITY of the
WESTERN CAPE

6.6 THE NEED FOR STATUTORY PROTECTION

Data protection under the right to privacy provides a blueprint for the protection of personal information under the right to property. The need for statutory protection of personal information arises due to the globalisation of economies, advancements in technology, and the ease of data movement, all of which pose difficulties to privacy from a data protection standpoint.[1322] However, these same factors facilitate the commodification of personal information, which presents challenges from a property perspective.

[1319] 2020 (4) SA 160 (GJ) para 68.4.
[1320] 2020 (4) SA 160 (GJ) para 68.5.
[1321] 2020 (4) SA 160 (GJ) para 88.
[1322] Burns Y & Burger-Smidt A (2023) 13–4. The shortcomings of the common law and constitutional protection with respect to data protection were highlighted in chapter three. See 3.2.1 and 3.2.2 above.

https://uwcscholar.uwc.ac.za/home

The enactment of data protection legislation, such as POPIA, the GDPR and the CCPA, has endowed personal information with certain property characteristics like excludability and alienability, founded on the premise that the collection and use are subject to the consent of data subjects.[1323] Therefore, it would be rational to augment the current data protection framework with a property framework to give effect to the constitutional right to property, which provides clarity as to ownership and property-based remedies, so as to foster the dignity and autonomy of the individual.[1324]

6.7 CONCLUSION

The notion of 'property' in s 25 has a potentially limitless scope. The incremental approach employed by the CC in determining whether a specific interest ought to be afforded protection under s 25 allows for flexibility with respect to future decision-making by the courts. As a result, the CC has been able to broaden the concept of constitutional property by recognising an increasing number of unconventional, intangible property rights and interests that are not typically considered property under private law.

In order to unlock the potential of the constitutional right to property, it is important to rely on the established principles of constitutional interpretation and to determine the scope of the term 'property' in the context of the Bill of Rights within which it is situated. A textual cum purposive cum contextual cum teleological interpretation is employed to inform our understanding of property. Such an interpretation requires a concept of property that leans towards a dynamic, public-law perspective rather than a private-law conceptualist understanding in order to reflect the evolving legal landscape and achieve its transformational potential.

The role of technology and its effects on personal information calls for a transformed mindset to meet the needs of a developing society. Personal information, by virtue of its very nature, is closely linked to dignity. The notion of property in s 25 is not only flexible to accommodate personal information, but that doing so promotes the dignity and autonomy of the individual.

[1323] See 4.10 above.
[1324] See the recommendations in 7.3 below.

https://uwcscholar.uwc.ac.za/home

CHAPTER SEVEN: CONCLUSION AND RECOMMENDATIONS

7.1 INTRODUCTION 213

7.2 CONCLUSIONS 213

7.2.1 What are the technological enablers of the personal information trade and the implications for the privacy of data subjects? 214

7.2.2 What entitlements do data subjects enjoy under South African data protection law, and are such entitlements effective given the personal information trade? 214

7.2.3 To what extent, given the commodification of personal information, could a property regime serve to regulate the use of resources? 216

7.2.4 In view of the commodification of personal information, could personal information be propertised in any sense? 217

7.2.5 Could personal information be recognised and protected for purposes of the South African constitutional property clause, and, if so, under what circumstances? 218

7.3 RECOMMENDATIONS 221

7.3.1 Scope of legislation 221

7.3.2 Scope of application 222

7.3.3 Proprietary rights in personal information 222

7.3.4 Consent 222

7.3.5 Opt-out 223

7.3.6 Security measures 223

7.3.7 Consideration 223

7.3.8 Remedies and sanctions 224

7.3.9 Registration of data processors and operators 224

7.3.10 Supervisory authority 224

7.4 SUGGESTIONS FOR FURTHER RESEARCH 225

UNIVERSITY of the WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

7.1 INTRODUCTION

This dissertation's central question is whether a constitutional conception of property can include personal information. The intention is to contribute to the academic literature in this field, particularly in South Africa, given the scarcity of such literature in this context. This main question entails several secondary questions, as outlined below. In contrast to the already existing literature, this dissertation considers an unconventional, intangible interest like personal information from a property perspective. This dissertation concludes that personal information could be protected as constitutional property, given its treatment as a commodity. First, the various conclusions made in this dissertation are summarised. Secondly, the chapter proposes guidelines for identifying personal information as a commodity and ensuring its protection under the constitutional property clause. Thirdly, the chapter suggests further areas of research that can be explored.

7.2 CONCLUSIONS

Chapter one identified and contextualised the research problem,[1325] formulated a central research question,[1326] and articulated five research sub-questions.[1327] In this regard, it was stated that technological improvements have led to the development of new business models centred around the processing of personal information. These new data practices drive economic activity while presenting new privacy challenges. Personal information has seemingly become an indispensable resource and a valuable commodity. Legal literature often addresses personal information in the context of privacy concerns or in the realm of data protection. However, the commodification of personal information demands a fresh perspective. It is submitted that the emergence of new assets challenges traditional legal conceptions of what property ought to be.

[1325] See 1.2 above.
[1326] See 1.2 above.
[1327] See 1.2 above.

https://uwcscholar.uwc.ac.za/home

7.2.1 What are the technological enablers of the personal information trade and the implications for the privacy of data subjects?

The dissertation in chapter two provided a discussion on the various technologies and its role in facilitating the collection and use of personal information.[1328] These technologies are known for their widespread observation of human behaviour, and they stand out for their capacity to gather data from various sources, analyse growing amounts of data for patterns and correlations, and produce insights about the data subjects. Importantly, technologies, comprising sensors and smart objects that are embedded in everyday objects, are working unobtrusively in the background without the knowledge of the data subject. The fact that these technologies are found in everyday objects implies that people are dependent on them for their daily routines; they may, however, not necessarily be aware of the data that is being collected and processed.

Data processing practices associated with such technologies raise several privacy concerns.[1329] These data practices undermine the freedom and autonomy of data subjects to make their own choices and decisions. However, looking beyond these privacy concerns, it is found that data practices are primarily concerned with extracting economic value from personal information. As a result, it makes it possible to transform personal information—traditionally seen as something non-commodifiable—into a valuable asset or commodity.

UNIVERSITY of the
WESTERN CAPE

7.2.2 What entitlements do data subjects enjoy under South African data protection law, and are such entitlements effective given the personal information trade?

Chapter three contained an analysis and commentary on the laws that govern data protection in South Africa at present. It was explained that the development of the South African law of privacy was channelled by a conception of privacy understood as secrecy.[1330] These common law principles were gradually incorporated into constitutional law jurisprudence over time, forming the basis of South African data protection law. The CC's privacy jurisprudence characterises privacy interests as lying on a spectrum. As interactions become more public, the expectation of privacy decreases but is not completely eliminated. However, technological

[1328] See 2.2 above.
[1329] See 2.3 above.
[1330] See 3.2.1 above.

https://uwcscholar.uwc.ac.za/home

developments have made such a privacy paradigm incompatible with contemporary data practices.

In addition to secrecy, control was also recognised as a fundamental element of South African data protection law.[1331] In response to the challenges posed by technological advancements, a control-based privacy paradigm provides individuals with better privacy protection than the limited, reactive data protection remedies provided by the common law and the Constitution. In this regard, the implementation of POPIA reflects a significant development in promoting the constitutional right to privacy.[1332] As such, data subjects are granted certain entitlements to control the processing of their personal information by others. However, the growing prevalence and complexity of commodification threaten data subjects' ability to maintain control over their personal information and their privacy under POPIA. This can be attributed to POPIA being designed to foster the privacy and dignity of data subjects, not the commodification of personal information.

At the same time, POPIA aims to minimise unnecessary impediments to the flow of data. A desire to ensure a free flow of data seems to suggest an economic dimension for implementing data protection regulations. This appears to contradict POPIA's other objective of maintaining privacy, an understanding of which is very much rooted in safeguarding the intimate personal sphere of individuals, and consequently, their dignity. This has no doubt contributed to the accretion of power in the private sector and encouraged the commodification of personal information. Therefore, private sector processing poses significant threats to the fundamental rights of data subjects. For this reason, it is necessary for the Constitution to apply to private relationships to ensure the interests of data subjects are protected. It was posited that the transformative nature of the Constitution provided a solid foundation for the development of legal principles capable of effectively addressing the challenges posed by modern-day information practices and the rising power of the private sector.[1333]

[1331] See 3.2.2 above.
[1332] See 3.3.3 above.
[1333] See 3.6 above.

https://uwcscholar.uwc.ac.za/home

7.2.3 To what extent, given the commodification of personal information, could a property regime serve to regulate the use of resources?

Chapter four explored the idea of establishing property rights in personal information in the US, where it was first proposed. The US is characterised by a regulatory environment that supports the trade in personal information, prioritises free-market principles, and encourages the sharing of personal information to promote economic growth and innovation.[1334] This is because the US roots privacy in liberty interests rather than individual dignity. In the US, the preference for a free flow of information over privacy protection makes it difficult to strike a balance between innovation and economic growth on the one hand and individual privacy on the other.

Therefore, the US typically implements data protection mechanisms to enable the free flow of data, with the protection of privacy being a secondary concern. The lack of cohesive data protection regulations creates an environment that encourages trade in personal information, leading to personal information being conceptualised in property terms to provide a better system for regulating its use. To this end, various economic-based property arguments have been proposed to regulate the use of personal information to ensure that there is no impediment to the free flow of information. These arguments propose allocating default entitlements to either the individuals associated with the personal information or the companies seeking to use it, the overall goal of which is to ensure the availability of information. The significance of these default entitlements is that they suggest elements of control that can be conceptualised in property terms, such as alienability and excludability.

Jurisdictions that prioritise the fundamental rights of individuals, such as South Africa and the EU, have also recognised the importance of a free flow of data. The realisation that a free flow of data is necessary for economic growth has undoubtedly contributed to personal information becoming a valuable economic resource. Therefore, it can be argued that human rights-framed data protection legislation, such as POPIA and the GDPR, has had little effect on changing the perspective of personal information as a commodity. Instead, jurisdictions, such as South Africa and the EU, must adopt and implement additional legal measures to deal with the commodification of personal information.

[1334] See 4.2 above.

UNIVERSITY of the WESTERN CAPE
https://uwcscholar.uwc.ac.za/home

7.2.4 In view of the commodification of personal information, could personal information be propertised in any sense?

Chapter five explored property rights in personal information from the EU perspective. As stated previously, the EU recognises the importance of a free flow of data to foster innovation, promote economic growth, and advance societal progress.[1335] In contrast to the US, data protection efforts in the EU are guided by human rights values.[1336] The EU recognises the right to data protection as a fundamental right alongside the right to privacy.[1337] As fundamental rights are inherently tied to individuals by reason of their personhood and are treated as non-commodifiable rights, it follows that personal information, as an aspect of data protection, is non-commodifiable.[1338] Therefore, different legislative mechanisms inside the EU, as shown below, demonstrate the clash between the view that personal information cannot be bought or sold and the actual fact that it is being bought and sold.

In order to balance economic growth with the protection of fundamental rights, the DSM strategy has implemented a number of regulatory initiatives to maximize the growth potential of the data economy in the EU.[1339] The GDPR is a regulatory mechanism that will play a central role in supporting the objectives of the DSM.[1340] A key feature of the GDPR is its strong commitment to fundamental rights and the protection of the right to data protection while ensuring a free flow of information. The understanding that personal information is not commodifiable is a cornerstone of the GDPR.

On the other hand, the Digital Content Directive, another important regulatory mechanism aimed at ensuring the proper functioning of the DSM, purports to recognise the commodification of personal information from the EU perspective in that it regulates the so-called 'free' business models involving the exchange of personal information for goods, thus implicitly recognising its economic value.[1341] This seemingly places the Digital Content Directive at odds with the GDPR insofar as it relates to the commodification of personal information. The question then arises as whether the GDPR can be interpreted in a way that

[1335] See 5.2 above.
[1336] See 5.1 above.
[1337] See 5.3 above.
[1338] See 5.1 above.
[1339] See 5.2 above.
[1340] See 5.3.3 above.
[1341] See 5.5 above.

https://uwcscholar.uwc.ac.za/home

could reconcile the apparently disparate legal positions adopted by the different regulatory instruments.

The GDPR does not expressly establish property-like protection in personal information.[1342] It is constructed along the lines of FIPs.[1343] In principle, the GDPR does not stipulate any monetary cost for the use and processing of personal information, nor does it envisage personal information as something that can be traded, exchanged or monetised. On the other hand, this may also be construed to mean that the GDPR does not explicitly preclude the adoption of a property framework as a regulatory tool.

The GDPR provides data subjects with a range of control and exclusion rights to strengthen their control over the processing of their personal information, which can be conceptualised in property terms. Such a conception of property can be understood in terms of a bundle of rights that make up ownership.[1344] When interpreted in this context, it suggests that the GDPR confers on data subjects a bundle of rights that constitute ownership to use and exclude others from using personal information.[1345]

Despite the EU persisting with the rhetoric that personal information is non-commodifiable, the actual situation in practice is very different. It is a fact that advances in technology and innovation have given rise to novel business models that make the commodification of personal information a distinct possibility. A human rights-based approach to privacy cannot alter or ignore the fact that the commodification of personal information does take place. Different jurisdictions may have divergent approaches to the treatment of personal information. However, a shared characteristic among all of them is the desire to extract economic value from such information.

7.2.5 Could personal information be recognised and protected for purposes of the South African constitutional property clause, and, if so, under what circumstances?

In South Africa, personal information is protected by data protection legislation, albeit not as property. Such protection stems from the constitutional right to privacy. However, given the phenomenon of commodification, there may be scope to include personal information under

[1342] See 5.4.1 above.
[1343] See 5.3.3.1 above.
[1344] See 5.5.2 above.
[1345] It is submitted that this would apply equally in the context of POPIA.

https://uwcscholar.uwc.ac.za/home

the constitutional property clause. In private law, the objective is to obtain property-like protection for private rights against competing private parties; the objective of constitutional law, on the other hand, is to ensure constitutional protection for an individual's private interests against the state or competing constitutional and other rights of other private parties. The concept of property under private law is inflexible since it is limited to the protection of corporeal things and real rights.[1346] Therefore, it is likely that the constitutional property concept will differ from the private law concept of property.[1347] The Constitution does not define the term 'property', but it could refer to either a legal object that is susceptible of ownership, whether tangible or intangible, or a range of rights and interests, both unconventional and traditional, real or personal. Therefore, it is possible for a wide range of rights and interests to qualify for constitutional property protection.

In a modern society, like South Africa, intangibles play an important role. Several intangible and information-based rights and interests have been accepted as constitutional property, despite such interests not being recognised as property in private law.[1348] Generally, these interests possess certain core features of property, such as economic value, alienability and excludability, which make them worthy of recognition and protection under the constitutional property clause.[1349] However, the fact that these interests may bear such property traits is no guarantee that such an interest will constitute property for the purposes of s 25 of the Constitution.

Determining whether a right or interest ought to be recognised as constitutional property requires an interpretation of s 25 that promotes the values that underlie an open and democratic society based on human dignity, equality, and freedom. Therefore, it cannot simply be accepted that the legal position of personal information as non-commodifiable is sacrosanct when viewed through a transformative lens. An interpretation of the constitutional concept of property ought to meet the needs of a developing society.

Failure to recognise the problem of commodification means a failure to properly protect the interests of data subjects, which in turn means they cannot enjoy the protections afforded to

[1346] Muller G et al *Silberberg and Schoeman's The Law of Property* 6 ed (2019) 10.

[1347] Du Bois M (2012) 178. Kellerman M *The Constitutional Property Clause and Immaterial Property Interests* (unpublished LLD thesis, University of Stellenbosch, 2011) 49–50 states that 'property' as understood under the constitutional property clause is broader than the private law concept and includes property interests recognised as property for private law purposes.

[1348] See 6.3 above.

[1349] See 6.5 above.

https://uwcscholar.uwc.ac.za/home

them under the Constitution. Recognising the tradability of information and its importance as an economic resource merits consideration of a legal regime that affords property protection.[1350] Excluding potential constitutional entitlements that may deserve protection under s 25 means that the Constitution will fail to meet the changing needs of society. The recognition of new kinds of constitutional property interests means that the concept of property is not static. The presence of distinct property attributes in personal information, such as economic value, transferability, and the ability to be excluded, provides further justification for its recognition as constitutional property. The recognition of personal information as a form of constitutional property reinforces the Constitution's relevance and power to transform society.

It is also recognised that personal information may differ from other types of incorporeal property. First, conventional property concepts, such as ownership and title, may be ill-suited when applied to personal information. However, the Constitution is concerned with property, not ownership.[1351] Moreover, nothing stops the adoption of legislation to allocate default entitlements, like ownership, in situations where personal information is deemed to be a commodity. Secondly, it is important to note that property characteristics may only become apparent in specific situations, since not all types of processing lead to the transformation of personal information into a commodity or the use of it as a means of trade. Property considerations ought to be triggered when there is an expectation of obtaining personal information through a contractual arrangement for economic purposes. For example, when individuals consent to their personal information being shared with a company in exchange for access to a product or service, the information so exchanged ought to be considered a form of property as it involves potential monetisation. Moreover, personal information may be considered property when it has commercial value, such as in the case of behavioural advertising or data analytics. In these situations, individuals ought to be entitled to some form of property rights over their personal information. Lastly, the fact that private law conceptions of property may not comfortably accommodate personal information does not justify its exclusion from constitutional property considerations.[1352]

[1350] Thomas M 'Information as property: Humanism or economic rationalism in the millenium?' (1998) 14 *Queensland University of Technology Law Journal* 203 203–13.
[1351] See 4.9.3 above.
[1352] See 6.6 above.

https://uwcscholar.uwc.ac.za/home

7.3 RECOMMENDATIONS

This section summarises the elements that ought to be incorporated in legislation to regulate the commodification of personal information. In this regard, please see the Appendix below for the draft Personal Information Commodities Bill, 2024, proposed as part of the recommendations that may be used as a blueprint for future legislation to be passed in South Africa. Since excludability can be established by way of legislation, it would be logical to assign property rights to personal information by way of legislation. Current data protection laws will serve as the foundation for this new legislation, which will establish a sui generis kind of property. Property rights will therefore only exist to the extent permitted by legislation,[1353] which will complement the existing data protection framework established through POPIA. This entails adopting a legislative approach similar to that of the EU, where a distinct statutory framework is established alongside the existing data protection legislation.

The objectives of such legislation would be (1) to designate personal information as a proprietary resource under limited circumstances, (2) grant default rights and entitlements, and (3) regulate the processing of personal information for the purposes of exchange and trade. As is the case with POPIA, the processing of personal information as a form of property ought to be based on similar legal principles to ensure the treatment of personal information as a commodity is lawful, fair and transparent.

UNIVERSITY of the
WESTERN CAPE

7.3.1 Scope of legislation

Legislation that gives effect to the constitutional right to property is required to establish clear guidelines for the ownership, use and transfer of personal information and to provide legal recognition and protection for personal information. By recognising the propertisation of personal information, such legislation aims to promote privacy, security, responsible use and accountability in the collection and use of personal information in a manner that fosters the dignity of the individual.

[1353] Karjiker S *Open-Source Software and the Rationale for Copyright Protection of Computer Programs* (unpublished LLD thesis, University of Stellenbosch, 2013) 10–20 points out that copyright and other forms of registered intellectual property exist because they are statutorily created. Moreover, intellectual property, as a form of property, exists because it is recognised as such by the state. See also Hazel S 'Personal Data as Property' (2020) 70 *Syracuse Law Review* 1055 1059.

https://uwcscholar.uwc.ac.za/home

7.3.2 Scope of application

The legislation creates a regulated personal data marketplace in terms of which a data subject (consumer) can consent to his or her personal information being shared with data merchants in exchange for access to online goods or services.[1354] The parties will enter into an agreement that aims to create a legal relationship between or among them in such a situation.

The legislation will also find application when a data merchant processes personal information of a consumer obtained through indirect means for the purposes of profiling and monetisation. Monetisation refers to the process of using personal information to obtain quantifiable economic benefit. Therefore, such processing will be subject to the legislation.

7.3.3 Proprietary rights in personal information

The default position is that personal information will be considered the property of the consumer to whom it relates.[1355] In other words, the consumer is the owner by default. The consumer will have the right to control the use, transfer and deletion of their personal information, subject to any limitations and conditions set forth in the legislation.

UNIVERSITY of the
WESTERN CAPE

7.3.4 Consent

The transfer of personal information from the consumer to a data merchant in terms of an agreement will require the express consent of the consumer.[1356] Such a transfer ought to be in the form of a non-exclusive licence agreement that is imposed by legislation.[1357] A licence approach conforms to the limited inalienability principle and guards against absurd situations arising, such as the irrevocable assignment of personal information to third parties. It would also be possible, in terms of a licence, to specify who has entitlements as to control, use and exclusion.

[1354] See generally ss 2, 3 and 6 of the Personal Information Commodities Bill below. Such an exchange would implicate consumer rights. However, such a discussion lies beyond the scope of this dissertation.
[1355] See generally s 5 of the Personal Information Commodities Bill below.
[1356] See s 7(a) of the Personal Information Commodities Bill below.
[1357] See s 6(a) of the Personal Information Commodities Bill below.

https://uwcscholar.uwc.ac.za/home

7.3.5 Opt-out

It was discussed in chapter two that most personal information is collected through indirect means without the knowledge of the consumer. It was further pointed out that this nullifies the effectiveness of the consent mechanism. Consequently, legislation ought to compel data merchants to inform affected consumers of the details of such processing to give consumers the opportunity to opt out.[1358] This would be particularly beneficial to consumers in those instances when parties obtain personal information through indirect means and use it for the purposes of profiling and monetisation. Compelling data merchants to inform consumers affords choice and ensures greater transparency as to how personal information is used, for what purpose and by whom. As a result, accountability for ensuring compliance with the regulatory framework rests with the data merchant.[1359]

7.3.6 Security measures

Data merchants must implement reasonable security measures to protect personal information from unauthorised access, disclosure, alteration or destruction.[1360]

7.3.7 Consideration

'Consideration' in this context refers to whether consumers ought to have the right to compensation for the use of their personal information. Given the economic value of personal information, it is likely that consumers ought to receive compensation for its use.[1361] Data

[1358] See s 5(c) of the Personal Information Commodities Bill below. The inclusion of an opt-out approach is an acknowledgement that not all personal information is collected through a consent process. Rather than rejecting it, as is currently the case with data protection legislation such as POPIA and the GDPR, an opt-out option can be used as an added measure to strengthen the control that data subjects have over the processing of their personal information by having it apply to personal information collected through data profiling techniques.

[1359] See ss7(c)–(f) of the Personal Information Commodities Bill below.

[1360] See ss 7(b) and 8 of the Personal Information Commodities Bill below.

[1361] Bottis M & Bouchagiar G 'Personal data v. Big data: Challenges of commodification of personal data' (2018) 8 *Open Journal of Philosophy* 206 208–9. Studies have already commenced to calculate the monetary value of personal data. See OECD 'Exploring the economics of personal data' 2013 4–6 available at *https://www.oecd–ilibrary.org/content/paper/5k486qtxldmq–en* (accessed 26 August 2019). The economic value of personal information is demonstrated by Shiru Coffee in Rhodes Island which allows students to exchange personal information for a free cup of coffee. See Empey C 'Is sharing personal data for free java worth the risk?' 11 October 2018 available at *https://blog.avast.com/shiru–cafe–offers–free–coffee–for–personal–data* (accessed 5 August 2021).

https://uwcscholar.uwc.ac.za/home

merchants' revenue streams from data-driven business models may further justify the consumer's right to compensation.[1362]

7.3.8 Remedies and sanctions

Under such legislation, consumers must have the right to seek legal recourse for any infringement of their rights. Data merchants who violate the provisions of such legislation ought to be subject to penalties, including fines and criminal sanctions.[1363]

7.3.9 Registration of data processors and operators

Data merchants, who will process personal information as envisaged in 7.3.2 will be obliged to register in terms of this legislation.[1364] The cabinet member responsible for overseeing the implementation of the legislation may, by notice in the Gazette, designate certain classes of data merchants to register. Registered users will be issued certificates (with or without conditions) for them to process information. If such users fail to comply with their statutory obligations, these certificates may be subject to periodic review and revocation or suspension. The purpose of such registration is to create conditions that can facilitate the controlled exchange of personal information and ensure that the commodification of such information occurs within a more regulated environment.

7.3.10 Supervisory authority

A supervisory authority, similar to the data protection authority established in terms of POPIA, ought to be created to oversee all data processing activities, monitor and enforce compliance under this legislation.[1365]

[1362] See s 6(a) of the Personal Information Commodities Bill below.
[1363] See ss 15–16 of the Personal Information Commodities Bill below.
[1364] See ss 11–14 of the Personal Information Commodities Bill below.
[1365] See ss 9–10 of the Personal Information Commodities Bill below.

https://uwcscholar.uwc.ac.za/home

7.4 SUGGESTIONS FOR FURTHER RESEARCH

The primary focus of this dissertation was to answer whether the notion of property in s 25 of the Constitution could be interpreted to accommodate personal data in a manner that underlies an open and democratic society based on the fundamental values of dignity, freedom and equality. Further research could be conducted to determine the circumstances under which the expropriation of personal information, as constitutional property, could occur, whether with or without compensation.

This dissertation focused exclusively on examining the privacy and commodification dimensions of personal data pertaining to individuals. It is suggested that further research could be conducted to explore the implications for juristic persons.

More research is required from a consumer protection law perspective because the commodification of personal data is now an established and widespread practice. This may require legislative reform, as the current South African consumer protection laws do not envisage personal data as something that can have monetary value or be used as a medium of exchange to acquire products and services.

Further research could be conducted to understand the implications if personal information constitutes a virtual currency that can be digitally traded and function as a medium of exchange, a unit of account, and/or a store of value from the perspective of the South African Reserve Bank.

UNIVERSITY of the
WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

APPENDIX: DRAFT PERSONAL INFORMATION COMMODITIES BILL, 2024

To regulate the processing of personal information in commercial transactions; to ensure respect for private property; and to provide for matters connected therewith.

BE IT ENACTED THEREFORE by the Parliament of the Republic of South Africa as follows:-

CHAPTER 1: DEFINITIONS AND PURPOSE (ss 1-3)

Definitions

1. In this Act, unless the context otherwise indicates, the following terms bear the meanings assigned thereto below –

'**Consent**' means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

'**Data consumer**' means the natural person to whom personal information relates;

'**Data controller**' means the party participating in a data marketplace that maintains the data consumer's data account and who controls access to personal information;

'**Data marketplace**' means an environment of networks where interdependent parties contribute to the collection, transfer and use of datasets, individualised or personalised, or that originate from individualised or personalised data, with a view to their distribution, sharing and processing through programming languages, algorithms, internet applications and processing infrastructure, data analysis, storage, and custody;

'**Data monetisation**' means the collection and analysis of personal information in order to create consumer profiles and target personalised advertising, develop products and services, identify behavioural patterns, and generate new sets of information of interest to those who acquire them, producing a quantifiable benefit for those who collect and process the personal information.

'**Data user**' means a private body which, alone or in conjunction with others, determines the purpose of and means for processing personal information, but does not include a data processor;

https://uwcscholar.uwc.ac.za/home

'**Data processor**' means the party who processes personal information for a registered entity user in terms of a contract or mandate and does not process the personal information for any of his own purposes;

'**Minister**' means the cabinet member responsible for the administration of justice;

'**Personal information**' means information relating to an identifiable, living, natural person, including but not limited to publicly available information, personal information relating to commercial transactions, consumer data and personal information related to financial transactions.

'**Processing**' means any operation or activity or any set of operations, or activity or set of operations, whether or not by automatic means, concerning personal information in connection with data monetisation;

'**Register**' means the repository of registered entities;

'**Registered entity**' means a data controller and/ or a data user as this case may be;

'**Registration**' means the registration of a data controller or a data user;

'**Regulator**' means the Data Property Regulator established in terms of section 9.

'**Republic**' means the Republic of South Africa.

UNIVERSITY of the
WESTERN CAPE

Purpose of Act

2. This Act aims to-

(a) establish a regulatory framework for personal information ownership and data monetisation;

(b) regulate the processing of personal information in a manner that is consistent with international standards;

(c) provide data consumers with rights and remedies to protect their personal information from processing that is not in accordance with this Act;

https://uwcscholar.uwc.ac.za/home

(d) establish a data marketplace that allows for the exchange of personal information in a manner that fosters the dignity and autonomy of data consumers.

3. Unless the context indicates otherwise, words importing the masculine gender include the feminine and neuter.

CHAPTER 2: APPLICATION PROVISIONS (s 4)

Application and interpretation of Act

4. (1) This Act applies to the processing of personal information-

(a) by any person who processes; and

(b) any person who had control over or authorises the processing of personal information for purposes of the data marketplace;

(c) where the data user is-

(i) domiciled in the Republic; or

(ii) not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.

(2)(a) This Act applies, subject to subsection (b), to the exclusion of any provision of any other legislation that regulates the processing of personal information and that is materially inconsistent with an object, or a specific provision, of this Act.

(b) If any other legislation provides for conditions for the lawful processing of personal information that are more extensive than those set out in this Act, the extensive conditions prevail to the extent that it does not conflict with the purpose of this Act.

CHAPTER 3: RIGHTS OF DATA CONSUMERS (s 5)

5. The data consumers shall have the right-

https://uwcscholar.uwc.ac.za/home

(a) to request from the data controller with whom his personal information was shared, a copy of such information that the data consumer has previously provided to the data controller, in a portable format and, to the extent technically feasible, easily usable, allowing the data consumer to transmit the data to another data controller without hindrance;

(b) to be notified of the identities of all other registered entities in the data marketplace with whom the personal information has been shared by the data controller along with a description of the personal information so shared;

(c) to opt-out of sharing his personal information or, at any time, not to share personal information related to transactions of any nature in which he participates;

(d) to correction, completion, updating and deletion of his personal information for the processing of which he has previously given consent;

(e) to approach the Regulator for redress in relation to the processing of his personal information or the exercise of his rights under the provisions of this Act.

UNIVERSITY of the
WESTERN CAPE

(f) to withdraw consent through the same channels in which it was given.

CHAPTER 4: REGULATING THE DATA MARKETPLACE (ss 6-8)

6. To ensure the proper functioning of the data marketplace-

(a) a registered entity that obtains personal information for the purposes of data monetisation must offer the data consumer, under the terms of a private contract, financial incentives or rewards, including payments as compensation for the collection, processing or sharing of personal information or information produced or made available by him in particular through access to and use of online electronic platforms, internet applications, marketplaces, portals and

https://uwcscholar.uwc.ac.za/home

websites, consumer relations, acquisition or sale of goods and services of any nature;

(b) registered entities participating in the data marketplace must register their participation in the register maintained through an electronic system, referred to in section 14;

(c) registered entities participating in the data marketplace are permitted to share personal information with other registered entities subject to section 7.

7. Sharing of personal information

(a) The data consumer consents to participating in the data marketplace by sharing his personal information with the data controller;

(b) Registered entities shall enter into an agreement with each other, pursuant to this Act, on aspects relating to:

(i) technological standards and operational procedures;
(ii) security standards;
(iii) requests from other registered entities to share personal information; and
(iv) the channels for forwarding requests from data consumers.

(c) A registered entity shall notify a data consumer that his personal information may be shared with other participants in the data marketplace and that data consumers have the right to opt-out of permission to share their data and personal information.

(d) A registered entity shall ensure that data consumers are provided with information in a clear, objective and appropriate manner with respect to shared data, which shall include:

(i) the identification of the participating entities;
(ii) the personal information being shared;

UNIVERSITY of the WESTERN CAPE
https://uwcscholar.uwc.ac.za/home

(iii) the period of validity of the consent;
(iv) the date on which consent was given; and
(v) the purpose of the consent.

(e) The data consumer shall be entitled to withdraw his consent by giving notice to through the appropriate channels provided by the data controller.

(f) Withdrawal of consent shall not affect any processing that occurred prior to such withdrawal.

8. Conditions for lawful processing

(a) A registered entity must ensure that processing complies with the following conditions:

(i) transparency;
(ii) adequate security measures and privacy of personal information;
(iii) data quality;
(iv) non-discriminatory treatment; and
(v) interoperability of systems.

UNIVERSITY of the
WESTERN CAPE

(b) Personal information processed by a data processor on behalf of a registered entity must:

(i) process such information only with the knowledge or authorisation of the registered entity; and

(ii) treat personal information which comes to their knowledge as confidential and must not disclose it,

unless required by law or in the course of the proper performance of their duties.

https://uwcscholar.uwc.ac.za/home

CHAPTER 5: SUPERVISION (ss 9-10)

9. There is hereby established a juristic person to be known as the Data Property Regulator, which-

(a) has jurisdiction throughout the Republic;

(b) is independent and is subject only to the Constitution and to the law and must be impartial and perform its functions and exercise its powers without fear, favour or prejudice;

(c) must exercise its powers and perform its functions in accordance with this Act and consider the Protection of Personal Information Act; and

(d) is accountable to the National Assembly.

10. Powers, duties and functions of the Regulator

The powers, duties and functions of the Regulator are the following:

(a) monitor and supervise compliance with the provisions of this Act, including the issuance of circulars, enforcement notices or any other instruments to any party;

(b) promote awareness and dissemination of information to the public about the operation of this Act;

(c) receive and investigate complaints about alleged infringements relating to the processing of personal information of data consumers and reporting to complainants in respect of such complaints;

(d) conduct research and to report to Parliament;

(e) consult with members of the public on any matter affecting the processing of personal information of a data consumer in terms of this Act;

(f) act as mediator between opposing parties on any matter that concerns the need for, or the desirability of, action by a registered entity relating to the processing of personal information of a data consumer;

https://uwcscholar.uwc.ac.za/home

CHAPTER 6: REGISTRATION (ss 11-14)

11. Registration of data controllers and data users

(a) The Minister may, upon the recommendation of the Regulator, publish in the Gazette, the category of data controllers and data users who shall be required to register under this Act.

(b) A party belonging to a category of data controllers or data users as specified in the order made under section 9(a) shall submit an application for registration to the Regulator in the manner and form as determined by the Regulator.

(c) After having given due consideration to an application under section 9(b), the Regulator may:

(i) register the applicant and issue a certificate of registration; or
(ii) refuse the application.

(d) The certificate of registration may be issued subject to such conditions or restrictions as the Regulator may deem fit to impose.

12. Renewal of certificate of registration

(a) A registered entity may make an application for the renewal of the certificate of registration not later than ninety days before the date of expiry of the certificate of registration in the manner and form as determined by the Regulator.

(b) When renewing a certificate of registration, the Regulator may vary the conditions or restrictions imposed upon the issuance of the certificate of registration or impose additional conditions or restrictions.

(c) The Regulator may refuse to renew a certificate of registration-

(i) if a registered entity has failed to comply with any of the provisions of this Act; or
(ii) if the registered entity has failed to comply with any of the conditions or restrictions imposed by the Regulator; or

https://uwcscholar.uwc.ac.za/home

(iii) the Regulator is satisfied that the registered entity is unable to continue the processing of personal information in accordance with this Act.

13. Revocation of registration

(a) The Regulator may revoke the registration of a registered entity if the Regulator is satisfied that-

(i) a registered entity has failed to comply with any of the provisions of this Act; or

(ii) a registered entity has failed to comply with any of the conditions or restrictions imposed by the Regulator; or

(iii) a registered entity is unable to continue the processing of personal information in accordance with this Act; or

(iv) a registered entity ceased to carry on the processing of personal information.

14. Register

(1) The Regulator shall maintain a register of registered entities.

UNIVERSITY of the
WESTERN CAPE

(2) The register shall contain the names and contact details of registered entities who have been registered pursuant to this Act.

(3) This register shall be available for public inspection.

CHAPTER 7: OFFENCES, PENALTIES AND FINES (ss 15-16)

Obstruction of Regulator

15. Any person who hinders, obstructs or unlawfully influences the Regulator or any person acting on behalf of or under the direction of the Regulator in the performance of the Regulator's duties and functions under this Act, is guilty of an offence.

https://uwcscholar.uwc.ac.za/home

Penalties

16(1) If the Regulator determines on conclusion of a complaint that breach of the provisions of this Act by a party is significant, it may, after giving the party an opportunity of being heard, impose a penalty up to the maximum amount as published by the Minister in the Gazette from time to time.

(2) While determining the amount of monetary penalty to be imposed under subsection (1), the Regulator shall have regard to the following matters, namely:

(a) the nature, gravity and duration of the breach;

(b) the type and nature of the personal information affected by the breach;

(c) repetitive nature of the breach;

(d) whether the party, as a result of the breach, has realised a gain or avoided any loss;

(e) whether the party took any action to mitigate the effects and consequences of the breach, and the timeliness and effectiveness of such action;

(f) whether the monetary penalty to be imposed is proportionate and effective, having regard to the need to secure observance of and deter breach of the provisions of this Act.

UNIVERSITY of the
WESTERN CAPE

CHAPTER 8: GENERAL (s 17)

17. Short title and commencement. – This Act is called the Personal Information Commodities Act, 2024 and comes into operation on a date to be determined by the President of the Republic of South Africa by proclamation in the Gazette

https://uwcscholar.uwc.ac.za/home

BIBLIOGRAPHY

1. BOOKS

Anglim J, Kirtley J & Nobahar G (eds) *Privacy Rights in the Digital Age (2015)* New York, US: Grey House Publishing

Britz H & Ackermann M *Information, Ethics & the Law* (2006) Pretoria: Van Schaik Publishers

Burns Y *Communications Law* 3 ed (2015) Durban: LexisNexis

Burns Y & Burger-Smidt A *Protection of Personal Information: Law and Practice* 2 ed (2023) South Africa: LexisNexis

Cachalia F & Klaaren J *Digitalisation, the 'Fourth Industrial Revolution' and the Constitutional Law of Privacy in South Africa: Towards a Public Law Perspective on Constitutional Privacy in the Era of Digitalisation* vol 14 (2021) Oxford: Digital Pathways at Oxford Paper Series

Currie I & De Waal J *The Bill of Rights Handbook* 6 ed (2013) Cape Town: Juta

De Stadler E & Esselaar *A Guide to the Protection of Personal Information Act* (2015) Cape Town: Juta

De Vos P & Freedman W (eds) *South African Constitutional Law in Context* (2014) Cape Town: Oxford University Press

Gutwirth S et al (eds) *Computers, Privacy and Data Protection: An Element of Choice* (2011) Dordrecht, Netherlands: Springer

Hildebrandt M *Law for Computer Scientists and Other Folk* (2020) UK: Oxford University Press

Hofman J et al *Cyberlaw A Guide for South Africans Doing Business Online* (1999) Cape Town: Ampersand Press

Kuner C et al (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press

Lessig L *Code Version 2.0* 2 ed (2006) New York: Basic Books

Lynskey O *The Foundations of EU Data Protection Law* (2015) Oxford: Oxford University Press

McQuoid-Mason D *The Law of Privacy in South Africa* (1978) Johannesburg: Juta

Moyle J *The Institutes of Justinian* 5 ed (1913) Oxford: Clarendon

Muller G et al *Silberberg and Schoeman's The Law of Property* 6 ed (2019) South Africa: LexisNexis

Neethling J & Potgieter J *Law of Delict* 8 ed (2021) South Africa: LexisNexis

https://uwcscholar.uwc.ac.za/home

Neethling J, Potgieter J & Visser P *Neethling's Law of Personality* 2 ed (2005) Durban: LexisNexis Butterworths

OECD *Data-Driven Innovation: Big Data for Growth and Well-Being* (2015) Paris: OECD Publishing

Solove D *The Digital Person: Technology and Privacy in the Information Age* (2004) New York: New York University Press

Tzanou M *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (2017) Oregon, US: Hart Publishing

Van der Merwe D et al *Information and Communications Technology Law* 2 ed (2016) Durban: LexisNexis

Van der Walt A *Property and Constitution* (2012) Pretoria: Pretoria University Law Press

Van der Walt A & Pienaar G *Introduction to the Law of Property* 7 ed (2016) Cape Town: Juta

Voigt A & Von dem Bussche A *The EU General Data Protection Regulation (GDPR): A Practical Guide* (2017) Switzerland: Springer International Publishing, Cham

Walters R, Trakman L & Zeller B *Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches* (2019) Singapore: Springer Nature Singapore Pte Ltd

Westin A *Privacy and Freedom* (1967) New York: Atheneum

Zimmerman R *The Law of Obligations: Roman Foundations of the Civilian Tradition* (1990) Cape Town: Juta

Zuboff S *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (2019) New York: PublicAffairs

UNIVERSITY of the
WESTERN CAPE

2. BOOK CHAPTERS

Andrade N 'Data protection, privacy and identity: Distinguishing concepts and articulating rights' in Fischer-Hűbner S et al (eds) *Privacy and Identity Management for Life. Privacy and Identity 2010. IFIP Advances in Information and Communication Technology* vol 352 (2010) Berlin: Springer

Cate F 'The failure of fair information practice principles' in Winn J (ed) *Consumer Protection in the Age of the Information Economy* (2006) Hampshire: Ashgate Publishing Ltd

Ciani J 'Governing data trade in intelligent environments: A taxonomy of possible regulatory regimes between property and access rights' in Chatzigiannakis I et al (eds) *Intelligent Environments* vol 23 (2018) Amsterdam: IOS Press

Custers B 'Data dilemmas in the information society: Introduction and overview' in Custers B et al (eds) *Discrimination and Privacy in the Information Society. Studies in Applied Philosophy, Epistemology and Rational Ethics* vol 3 (2013) Berlin: Springer

https://uwcscholar.uwc.ac.za/home

Custers B & Schermer B 'Responsibly innovating data mining and profiling tools: A new approach to discrimination sensitive and privacy sensitive attributes' in Van den Hoven J et al (eds) *Responsible Innovation 1: Innovative Solutions for Global Issues* (2014) Dordrecht: Springer

De Franceschi A 'Personal data as counter-performance' in Senigaglia R, Irti C & Bernes A (eds) *Privacy and Data Protection in Software Services, Services and Business Process Reengineering* (2022) Singapore: Springer Nature Singapore Pte Ltd

De Hert P & Lammerant H 'Predictive profiling and its legal limits: Effectiveness gone forever?' in Van der Sloot B, Broeders D & Schrijvers E (eds) *Exploring the Boundaries of Big Data* (2016) Amsterdam: Amsterdam University Press

DeCew J 'Privacy' in Zalta E (ed) *The Stanford Encyclopedia of Philosophy* (Spring 2018) Stanford, California: Metaphysics Research Lab, Stanford University available at *https://plato.stanford.edu/archives/spr2018/entries/privacy/* (accessed 6 October 2020)

Erlank W 'Law and Property in Virtual Worlds' in Barfield W & Blitz M (eds) *Research Handbook on the Law of Virtual and Augmented Reality* (2018) Cheltenham, United Kingdom: Edward Elgar Publishing Limited

Gürses S & Preneel B 'Cryptology and privacy in the context of big data' in Van der Sloot B, Broeders D & Schrijvers E (eds) *Exploring the boundaries of big data* (2016) Amsterdam: Amsterdam University Press

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

Haynes P and Carolyn Nguyen M 'Rebalancing socioeconomic asymmetry in a data-driven economy' in Bilao-Osorio B, Dutta S & Lanvin B (eds) *The Global Technology Report 2014: Rewards and risks of big data* (2014) Geneva: World Economic Forum and INSEAD

Hildebrandt M 'Defining profiling: A new type of knowledge?' in Hildebrandt M & Gutwirth S (eds) *Profiling the European Citizen: Cross-Disciplinary Perspectives* (2008) New York: Springer

Hildebrandt M & Gutwirth S 'General introduction and overview' in Hildebrandt M & Gutwirth S (eds) *Profiling the European Citizen: Cross-Disciplinary Perspectives* (2008) New York: Springer

Lawack V, Kaseke M & Fransman M 'Consumer protection law aspects of cryptoassets' in Lawack V (ed) *Fintech Law and Regulation: An African Perspective* (2023) Cape Town: Juta

McQuoid-Mason D 'Chapter 38: Privacy' in Woolman S & Bishop M (eds) *Constitutional Law of South Africa* 2 ed (Revision Service 6) Cape Town: Juta

Neethling J 'Appropriation of competitor's business ideas: Acquisition and use of competitor's trade secrets or confidential information; Misappropriation of competitor's performance' in Van Heerden H & Neethling J (eds) *Unlawful competition* 2 ed (2008) Durban: LexisNexis

https://uwcscholar.uwc.ac.za/home

Prins C 'Property and privacy: European perspectives and the commodification of our identity' in Guibault L & Hugenholtz P (eds) *The Future of the Public Domain* (2006) The Hague, Netherlands: Kluwer Law International

Purtova N 'Property in personal data: Second life of an old idea in the age of cloud computing, chain informatisation, and ambient intelligence' in Gutwirth S et al (eds) *Computers, Privacy and Data Protection: an Element of Choice* (2011) Dordrecht: Springer

Rouvroy A & Poullet Y 'The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy' in Gutwirth S et al (eds) *Reinventing Data Protection?* (2009) Dordrecht: Springer

Ruiter J & Warnier M 'Privacy regulations for cloud computing: compliance and implementation in theory and practice' in Gutwirth S et al (eds) *Computers, Privacy and Data Protection: an Element of Choice* (2011) Dordrecht: Springer

Snail S & Papadopoulos S 'Privacy and data protection' in Papadopoulos S & Snail S (eds) *Cyberlaw@SA IV: the law of the Internet in South Africa* 4 ed (2022) Pretoria: Van Schaik Publishers

Strowel A 'Big Data and data appropriation in the EU' in Aplin T (ed) *Research Handbook on Intellectual Property and Digital Technologies* (2020) Cheltenham, United Kingdom: Edward Elgar Publishing Limited

Tavani H 'Informational privacy: Concepts, theories, and controversies' in Himma H & Tavani H (eds) *The Handboook of Information and Computer Ethics* (2008) New Jersey: John Wiley and Sons Inc

Taylor L 'Safety in numbers? Group privacy and big data analytics in the developing world' in Taylor L, Floridi L & Van der Sloot B (eds) *Group Privacy: New Challenges of Data Technologies* vol 126 (2017) Cham, Switzerland: Springer

Taylor L, Floridi L & Van der Sloot B 'Introduction: A new perspective on privacy' in Taylor L, Floridi L & Van der Sloot B (eds) *Group Privacy: New Challenges of Data Technologies*, vol 126 (2017) Cham, Switzerland: Springer

Van den Hoven J et al 'Privacy and information technology' in Zalta E (ed) *The Stanford Encyclopedia of Philosophy* (Summer 2020) Stanford, California: Metaphysics Research Lab, Stanford University available at https://plato.stanford.edu/archives/sum2020/entries/it–privacy/ (accessed 9 July 2020)

Van der Sloot B 'Legal fundamentalism: Is data protection really a fundamental right?' in Leenes R et al (eds) *Data Protection and Privacy: (In)visibilities and Infrastructures* vol 36 (2017) Cham: Switzerland: Springer International Publishing

Van Hoboken J 'From collection to use in privacy regulation? A forward-looking comparison of European and US frameworks for personal data processing' in Van der Sloot B, Broeders D & Schrijvers E (eds) *Exploring the Boundaries of Big Data* (2016) Amsterdam: Amsterdam University Press

Van Lieshout M 'The value of personal data' in Aspinall D et al (eds) *Privacy and Identity*, vol 457 (2014) Berlin: Springer

https://uwcscholar.uwc.ac.za/home

Van Zyl E, De Stadler E & Eiselen S 'Section 11' in Naude T & Eiselen S (eds) *Commentary on the Consumer Protection Act* (2014) Jutastat e-publications

3. CONFERENCE PRESENTATIONS AND RESEARCH PAPERS

De Mauro A, Greco M & Grimaldi M *What Is Big Data? A Consensual Definition and a Review of Key Research Topics* (2015) AIP Conference Proceedings

Falch M *Surveillance Capitalism - a New Techno-Economic Paradigm?* (2020) 13th CMI Conference on Cybersecurity and Privacy (CMI) - Digital Transformation - Potentials and Challenges

Könings B & Schaub F *Territorial Privacy in Ubiquitous Computing* (2011) Eighth International Conference on Wireless On-Demand Network Systems and Services

Lessig L '*The Architecture of Privacy* (1998) Taiwan Net, Taipei

Lukács A *What Is Privacy? The History and Definition of Privacy* (2016) University of Szeged, Faculty of Law and Political Sciences

Malgieri G *The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation* (2020) Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, Association for Computing Machinery

Polykalas S et al *Mobile Apps and Data Privacy: When the Service Is Free, the Product Is Your Data* (2017) 8th International Conference on Information, Intelligence, Systems Applications, Larnaca

UNIVERSITY of the
WESTERN CAPE

4. DISSERTATIONS (SOUTH AFRICAN UNIVERSITIES)

Allotey A *Data Protection and Transborder Data Flows: Implications for Nigeria's Integration into the Global Network Economy* (unpublished LLD thesis, University of South Africa, 2014)

Dean O *The Application of the Copyright Act, 1978, to Works Made Prior to 1979* (unpublished LLD thesis, University of Stellenbosch, 1988)

Donnelly D *Privacy by (Re)Design: A Comparative Study of the Protection of Personal Information in the Mobile Applications Ecosystem under United States, European Union and South African Law* (unpublished LLD thesis, University of KwaZulu-Natal, 2020)

Erlank W *Property in Virtual Worlds* (unpublished LLD thesis, University of Stellenbosch, 2012)

Karjiker S *Open-Source Software and the Rationale for Copyright Protection of Computer Programs* (unpublished LLD thesis, University of Stellenbosch, 2013)

Kellerman M *The Constitutional Property Clause and Immaterial Property Interests* (unpublished LLD thesis, University of Stellenbosch, 2011)

https://uwcscholar.uwc.ac.za/home

Lawack V *Aspects of Internet Payment Instruments* (unpublished LLD thesis, University of South Africa, 2001)

Njotini M *E-Crimes and E-Authentication – Legal Perspective* (unpublished LLD thesis, University of South Africa, 2016)

Roos A '*The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* (unpublished LLD thesis, University of South Africa, 2003)

5. DISSERTATIONS (FOREIGN UNIVERSITIES)

Li W *Data Portability as a New Means of Data Protection? Examining the Right to Data Portability in the EU General Data Protection Regulation* (unpublished PhD thesis, University of Edinburgh, 2019)

Purtova N *Property Rights in Personal Data* (published PhD thesis, Tilburg University, 2011)

6. INTERNET MATERIAL

Author unknown 'The Netflix prize rules' (undated) available at *https://netflixprize.com/assets/rules.pdf* (accessed 4 September 2020)

Banafa A 'The Internet of everything (IoE)' 29 August 2016 available at *https://www.bbvaopenmind.com/en/technology/digital–world/the–internet–of–everything–ioe/* (accessed 6 August 2020)

Barbaro M & Jr T 'A face is exposed for AOL Searcher No. 4417749' *The New York Times* 9 August 2006 available at *https://www.nytimes.com/2006/08/09/technology/09aol.html* (accessed 4 September 2020)

Bellamy F 'US Data privacy laws to enter new era in 2023' *Reuters* 12 January 2023 available at *https://www.reuters.com/legal/legalindustry/us–data–privacy–laws–enter–new–era–2023–2023–01–12/* (accessed 4 August 2023)

Cadwalladr C & Graham-Harrison E 'Revealed: 50 Million Facebook profiles harvested for Cambridge Analytica in Major Data Breach' *The Guardian* 17 March 2018 available at *https://www.theguardian.com/news/2018/mar/17/cambridge–analytica–facebook–influence–us–election* (accessed 27 February 2021)

Dang S et al 'Exclusive: AT&T considers cellphone plans subsidized by ads' *Reuters* 16 September 2020 available at *https://www.reuters.com/article/us–at–t–ceo–interview–exclusive/exclusive–att–considers–cellphone–plans–subsidized–by–ads–idUSKBN2663HK* (accessed 14 March 2023)

Deutsch A 'The 5 Industries driving the US economy' *Investopedia* 17 September 2020 available at *https://www.investopedia.com/articles/investing/042915/5–industries–driving–us–economy.asp* (accessed 26 September 2020)

https://uwcscholar.uwc.ac.za/home

Empey C 'Is sharing personal data for free java worth the risk?' 11 October 2018 available at *https://blog.avast.com/shiru–cafe–offers–free–coffee–for–personal–data* (accessed 5 August 2021)

Facebook 'An Update on Our Plans to Restrict Data Access on Facebook' 4 April 2018 available at *https://about.fb.com/news/2018/04/restricting-data-access/* (accessed 28 February 2021)

Freedman M 'How and why businesses collect your personal data' *Business News Daily* 17 June 2020 available at *https://www.businessnewsdaily.com/10625–businesses–collecting–data.html* (accessed 25 February 2021)

FXSSI 'Most valuable companies in the world – 2022' 27 July 2022 available at *https://fxssi.com/top–10–most–valuable–companies–in–the–world* (accessed 7 November 2022)

Gallie A 'The General Data Protection Regulation – A two–year retrospective' 22 May 2020 available at *https://www.lexology.com/library/detail.aspx?g=71abd6e1–83d6–4cf1–b807–fe6ef1565b6a* (accessed 4 March 2022)

Google 'Privacy Policy – Privacy & Terms' 4 March 2024 available at *https://policies.google.com/privacy* (accessed 20 March 2024)

i-SCOOP 'What the internet of everything really is – a deep dive' (undated) available at *https://www.i–scoop.eu/internet–of–things–guide/internet–of–everything/* (accessed 6 August 2020)

Insights Association 'Behavioral targeting' (undated) available at *https://www.insightsassociation.org/issues–policies/glossary/behavioral–targeting* (accessed 7 September 2020)

Kuneva M 'Roundtable on online data collection, targeting and profiling' 31 March 2009 available at *https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156* (accessed 16 March 2020)

Marr B 'Here's why data is not the new oil' 6 June 2019 available at *https://www.forbes.com/sites/bernardmarr/2018/03/05/heres–why–data–is–not–the–new–oil/#7650084f3aa9* (accessed 6 June 2019)

Mtweve E 'Data as Property (Article 7)' 16 August 2022 available at *https://victoryattorneys.co.tz/data-as-property-article-7/* (accessed 22 December 2023)

OECD 'Exploring the economics of personal data' (undated) available at *https://www.oecd–ilibrary.org/content/paper/5k486qtxldmq–en* (accessed 26 August 2019)

Privacy International 'Data is power: profiling and automated decision-making in GDPR' 2018 available at *https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr* (accessed 10 September 2020)

Privacy International 'Big data' 8 February 2018 available at *http://privacyinternational.org/explainer/1310/big–data* (accessed 24 August 2020)

https://uwcscholar.uwc.ac.za/home

Privacy Rights Clearinghouse 'The privacy implications of cloud computing' 2017 available at *https://privacyrights.org/resources/privacy–implications–cloud–computing* (accessed 27 July 2020)

Propato M & Zannoni L 'The Debate over Data Monetization – an EU (and Italian) Perspective' 13 June 2022 available at *https://www.dentons.com/en/insights/articles/2022/june/13/the-debate-over-data-monetization-an-eu-and-italian-perspective* (accessed 24 May 2024)

Rosenberg M Confessore N & Cadwalladr C 'How Trump consultants exploited the facebook data of millions' *The New York Times* 17 March 2018 available at *https://www.nytimes.com/2018/03/17/us/politics/cambridge–analytica–trump–campaign.html* (accessed 27 February 2021)

Rouse M 'Ubiquitous computing' *Technopedia* 18 March 2014 available at *https://www.techopedia.com/definition/22702/ubiquitous–computing* (accessed 12 April 2023)

Sager M 'Andy Grove: What I've learned' *Esquire* 2007 available at *https://www.esquire.com/features/what–ive–learned/learned–andy–grove–0500* (accessed 9 July 2020)

Shapiro R and Aneja S 'Who Owns Americans' Personal Information and What Is It Worth? - Future Majority' 2019 available at *https://www.futuremajority.org/pages/who-owns-americans-personal-information* (accessed 29 April 2020)

South African Reserve Bank 'Position paper on virtual currencies position paper' available at *https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014* (accessed 22 August 2019)

The Economist 'The world's most valuable resource is no longer oil, but data' (6 May 2017) available at *https://www.economist.com/leaders/2017/05/06/the–worlds–most–valuable–resource–is–no–longer–oil–but–data* (accessed 6 June 2019)

Viljoen S 'The promise and pitfalls of the California Consumer Privacy Act' (2020) available at *https://www.dli.tech.cornell.edu/post/the–promise–and–pitfalls–of–the–california–consumer–privacy–act* (accessed 15 December 2020)

7. JOURNAL ARTICLES

Abdulrauf L & Fombad C 'The African Union's data protection convention 2014: A possible cause for celebration of human rights in Africa?' (2016) 8 *Journal of Media Law* 67–97

Abdulrauf L & Fombad C 'Personal data protection in Nigeria: Reflections on opportunities, options and challenges to legal reforms' (2017) 38 *Liverpool Law Review* 105–34

Abril P 'Recasting privacy torts in a spaceless world' (2007) 21 *Harvard Journal of Law and Technology* 1–47

https://uwcscholar.uwc.ac.za/home

Alibeigi A, Munir A & Ershadul Karim M 'Right to privacy, a complicated concept to review' (2019) *Library Philosophy and Practice* 1–36

Allen A 'Privacy-as-data control: Conceptual, practical, and moral limits of the paradigm' (2000) 32 *Connecticut Law Review* 861–76

Altman M et al 'Practical approaches to big data privacy over time' (2018) 8 *International Data Privacy Law* 29–51

Aretz Y & Strandburg K 'Privacy regulation and innovation policy' (2020) 22 *Yale Journal of Law and Technology* 256–317

Aretz Y & Strandburg K 'Regulation and innovation: Approaching market failure from both sides' (2020) *Yale Journal on Regulation* 1–27

Azarchs T 'Informational privacy: Lessons from across the atlantic' (2014) 16 *Journal of Constitutional Law* 805–34

Baik J 'Data Privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA)' (2020) 52 *Telematics and Informatics* 1–10

Baker E 'Trustless property systems and anarchy: How trustless transfer technology will shape the future of property exchange' (2015) 45 *Southwestern Law Review* 351–76

Bandara R, Fernando M & Akter S 'The privacy paradox in the data-driven marketplace: The role of knowledge deficiency and psychological distance' (2017) 121 *Procedia Computer Science* 562–67

Baron J 'Property as control: The case of information' (2012) 18 *Michigan Telecommunications and Technology Law Review* 367–418

Batchelor B & Wazvaremhaka T 'Balancing financial inclusion and data protection in South Africa: Black Sash Trust v Minister of Social Development' (2019) 136 *SALJ* 112–30

Bedir C 'Contract law in the age of big data' (2020) 16 *European Review of Contract Law* 347–65

Bennet S 'Regulating online behavioral advertising' (2011) 44 *The John Marshall Law Review* 899–962

Bentley D 'Timeless principles of taxpayer protection: How they adapt to digital disruption' (2019) 16 *eJournal of Tax Research* 679–713

Bergelson V 'It's personal but is it mine? Toward property rights in personal information' (2003) 37 *University of California Davis Law Review* 379–451

Berger D 'Balancing consumer privacy with behavioral targeting' (2010) 27 *Santa Clara High Technology Law Journal* 3–61

Betzing J et al 'The impact of transparency on mobile privacy decision making' (2020) 30 *Electronic Markets* 607–25

https://uwcscholar.uwc.ac.za/home

Bhagwat A 'Sorrell v. IMS Health: Details, detailing, and the death of privacy' (2012) 36 *Vermont Law Review* 855–80

Bilchitz D 'Privacy, surveillance and the duties of corporations' (2016) 1 *TSAR* 45–67

Boerding A et al 'Data ownership—A property rights approach from a European perspective' (2018) 11 *Journal of Civil Law Studies* 323–69

Boerman S, Kruikemeier S & Zuiderveen Borgesius F 'Online behavioral advertising: A literature review and research agenda' (2017) 46 *Journal of Advertising* 363–76

Bottis M & Bouchagiar G 'Personal data v. Big data: Challenges of commodification of personal data' (2018) 8 *Open Journal of Philosophy* 206–15

Bredican J & Ellis D 'Smartphone applications - Idea sourcing, and app development: implications for firms' (2014) 17 *SAJEMS* 232–48

Brenner S 'Privacy privilege: Law enforcement, technology, and the Constitution' (2002) 7 *Journal of Technology Law & Policy* 123–94

Brkan M 'The unstoppable expansion of the EU fundamental right to data protection: Little shop of horrors?' (2016) 23 *Maastricht Journal of European and Comparative law* 812–41

Bruckner M 'The promise and perils of algorithmic lenders' use of big data' (2018) 93 *Chicago-Kent Law Review* 3–60

Buchanan T et al 'Development of measures of online privacy concern and protection for use on the Internet' (2007) 58 *Journal of the American Society for Information Science and Technology* 157–65

Bühler S 'Conditional consent as a valid legal ground for data processing - a misbelief?' (2019) *Freiburg Law Students Journal* 25–31

Burchell J 'The legal protection of privacy in South Africa: A transplantable hybrid' (2009) 13 *Electronic Journal of Comparative Law* 1–26

Buttarelli G 'The EU GDPR as a clarion call for a new global digital gold standard' (2016) 6 *International Data Privacy Law* 77–8

Calabresi G & Melamed D 'Property rules, liability rules, and inalienability: One view of the cathedral' (1972) 85 *Harvard Law Review* 1089–128

Cate F 'Principles of internet privacy' (2000) 32 *Connecticut Law Review* 877–96

Cate F & Cate B 'The Supreme Court and information privacy' (2012) 2 *International Data Privacy Law* 255–67

Cate F & Litan R 'Constitutional issues in information privacy' (2002) 9 *Michigan Telecommunications and Technology Law Review* 35–63

Chemerinsky E 'Substantive due process' (1999) 15 *Touro Law Review* 1501–534

UNIVERSITY of the WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

Cheneval F 'Property rights of personal data and the financing of pensions' (2018) *Critical Review of International Social and Political Philosophy* 1–23

Chidede T 'The role of intellectual property rights' protection in advancing development in South Africa' (2022) 26 *Law, Democracy & Development* 168–89

Chirwa D 'The horizontal application of constitutional rights in a comparative perspective' (2006) 10 *Law, Democracy & Development* 21–48

Cofone I 'The dynamic effect of information privacy law' (2017) 18 *Minnesota Journal of Law, Science & Technology* 517–74

Cohen J 'Examined lives: Informational privacy and the subject as object' (2000) 52 *Stanford Law Review* 1373–437

Cohen J 'What privacy is for' (2013) 126 *Harvard Law Review* 1904–933

Cornelius S 'Commercial appropriation of a person's image: Wells v Atoll Media (Pty) Ltd (Unreported 11961/2006) [2009] ZAWCHC 173 (9 November 2009)' (2011) 14 *PELJ* 182–205

Crawford K & Schultz J 'Big data and due process: Toward a framework to redress predictive privacy harms' (2014) 55 *Boston College Law Review* 93–128

Cuipers C 'A private law approach to privacy; mandatory law obliged?' (2007) 4 *SCRIPTed* 304–18

Cunningham M 'Next generation privacy: The Internet of Things, data exhaust, and reforming regulation by risk of harm' (2014) 2 *Groningen Journal of International Law* 115–44

Custers B & Malgieri G 'Priceless data: Why the EU fundamental right to data protection is at odds with trade in personal data' (2022) 45 *Computer Law & Security Review* 1–11

Custers B & Ursic H 'Big data and data reuse: A Taxonomy of data reuse for balancing big data benefits and personal data protection' (2016) *International Data Privacy Law* 1–12

De Hert P et al 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services' (2018) *Computer Law and Security Review* 193–203

De Hert P & Sajfert J 'Regulating big data in and out of the data protection policy field: Two scenarios of post-GDPR law-making and the actor perspective' (2019) 5 *European Data Protection Law Review* 338–51

De Hingh A 'Some reflections on dignity as an alternative legal concept in data protection regulation' (2018) 19 *German Law Journal* 1269–290

De Montjoye Y et al 'Unique in the crowd: The privacy bounds of human mobility' (2013) *Scientific Reports* 1–5

Del Rosario L 'On the propertization of data and the harmonization imperative' (2022) 90 *Fordham Law Review* 1699–742

https://uwcscholar.uwc.ac.za/home

Donald M 'Unlocking the potential of wellbeing in the environmental right: A teleological interpretation' (2020) 31 *Stellenbosch Law Review* 55–79

Douglas-Scott S 'The European Union and human rights after the Treaty of Lisbon' (2011) 11 *Human Rights Law Review* 645–82

Du Bois M 'Intellectual property as a constitutional property right: The South African approach' (2012) 24 *SA Mercantile Law Journal* 177–93

Durovic M & Montanaro M 'Data protection and data commerce: Friends or foes?' (2021) 17 *European Review of Contract Law* 1–36

Eades R 'Attempts to federalize and codify tort law' (2000) 36 *American Bar Association* 1– 21

Efroni Z 'Gaps and opportunities: The rudimentary protection for "data-paying consumers" under new EU consumer protection law' (2020) 57 *Common Market Law Review* 799–830

Eggers W, Hamill R & Ali A 'Data as the new currency: Government's role in facilitating the exchange' (2013) 13 *Deloitte Review* 18–31

Elvy S 'Commodifying consumer data in the era of the Internet of Things' (2018) 59 *Boston College Law Review* 423–522

Erlank W 'Introduction to Virtual Property: Lex Virtualis Ipsa Loquitur' (2015) 18 *PELJ* 2525–559

Fayyad U, Piatetsky-Shapiro G & Smyth P 'From data mining to knowledge discovery in databases' (1996) 17 *AI Magazine* 37–54

Felzmann H et al 'Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns' (2019) *Big Data and Society* 1–14

Finck M & Pallas F 'They who must not be identified-distinguishing personal from non-personal data under the GDPR' (2020) 10 *International Data Privacy Law* 11–36

Forde A 'Implications of the right to be forgotten' (2015) 18 *Tulane Journal of Technology and Intellectual Property* 83–131

Friedewald M & Pohoryles R 'Technology and privacy' (2013) 26 Innovation: *The European Journal of Social Science Research* 1–6

Froomkin M 'From anonymity to identification' (2015) 1 *Journal of Self-Regulation and Regulation* 120–38

Froomkin M 'Big data: Destroyer of informed consent' (2019) 21 *Yale Journal of Law and Technology* 27–54

Garry P 'Liberty through limits: The Bill of Rights as limited government provisions' (2009) 62 *SMU Law Review* 1745–782

Gilbert H 'Minors' constitutional right to informational privacy' (2007) 74 *University of Chicago Law Review* 1375–410

https://uwcscholar.uwc.ac.za/home

Gillis T & Spiess J 'Big data and discrimination' (2019) 86 *University of Chicago Law Review* 459–87

Goldfarb A & Tucker C 'Privacy and innovation' (2012) 12 *Innovation Policy and the Economy* 65–90

González Fuster G & Gellert R 'The fundamental right of data protection in the European Union: In search of an uncharted right' (2012) 26 *International Review of Law, Computers & Technology* 73–82

González Fuster G & Gutwirth S 'Opening up personal data protection: A conceptual controversy' (2013) 29 *Computer Law & Security Review* 531–39

Gorkin R 'The constitutional right to informational privacy: NASA v Nelson' (2010) 6 *Duke Journal of Constitutional Law & Public Policy Sidebar* 1–20

Graef I, Husovec M & Purtova N 'Data portability and data control: lessons for an emerging concept in EU law' (2018) 19 *German Law Journal* 1359–398

Gray K 'Property in thin air' (1991) 50 *Cambridge Law Journal* 252–307

Gruschka N et al 'Privacy issues and data protection in big data: A case study analysis under GDPR' (2018) *IEEE International Conference on Big Data* 5027–33

Hagemann R, Skees J & Thierer A 'Soft law for hard problems: The governance of emerging technologies in an uncertain future' (2018) 17 *Colorado Technology Law Journal* 37–130

Harbinja E 'Does the EU data protection regime protect post-mortem privacy and what could be the potential alternatives?' (2013) 10 *SCRIPTed* 19–38

Hartzog W 'The inadequate, invaluable fair information practices' (2017) 76 *Maryland Law Review* 952–83

Hasan O et al 'A discussion of privacy challenges in user profiling with big data techniques: The EEXCESS use case' (2013) *IEEE International Congress on Big Data* 25–30

Hazel S 'Personal data as property' (2020) 70 Syracuse Law Review 1055–114

Helberger N, Zuiderveen Borgesius F & 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* 1427–465

Hildebrandt M 'Profiling: From data to knowledge' (2006) 30 *Datenschutz und Datensicherheit - DuD* 548–52

Hildebrandt M 'Profiling and the rule of law' (2008) 1 *Identity in the Information Society* 55–70

Hohfeld W 'Fundamental legal conceptions as applied in judicial reasoning' (1917) 26 *Yale Law Journal* 710–70

https://uwcscholar.uwc.ac.za/home

Hoofnagle C, Van der Sloot B & Zuiderveen Borgesius F 'The European Union General Data Protection Regulation: What it is and what it means' (2019) 28 *Information & Communications Technology Law* 65–98

Hoofnagle C & Whittington J 'Free: Accounting for the costs of the internet's most popular price' (2013) 61 *University of California Law Review* 606–70

Hu M 'Cambridge Analytica's black box' (2020) *Big Data and Society* 1–6

Hummel P, Braun M & Dabrock P 'Own data? Ethical reflections on data ownership' (2020) *Philosophy & Technology* 545–72

Jacoby N 'Redefining the right to be let alone: Privacy rights and the constitutionality of technical surveillance measures in Germany and the United States' (2007) 35 *Georgia Journal of International and Comparative Law* 435–93

Janeček V 'Ownership of personal data in the Internet of Things' (2018) 34 *Computer Law & Security Review* 1039–52

Janeček V & Malgieri G 'Commerce in data and the dynamically limited alienability rule' (2020) 21 *German Law Journal* 924–43

Jerome J 'Big Data: Catalyst for a privacy conversation' (2014) 48 *Indiana Law Review* 213–42

Jin H et al '"Why are they collecting my data?": Inferring the purposes of network traffic in mobile apps' (2018) 2 *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1–27

Kang J 'Information privacy in cyberspace transactions' (1998) 50 *Stanford Law Review* 1193–294

Karjiker S 'Justifications for copyright: The economic justifications' (2014) 4 *South African Intellectual Property Law Journal* 13–41

Kelly R & Swaby G 'Consumer protection rights and "free" digital content' (2017) 23 *Computer and Telecommunications Law Review* 165–70

King N & Forder J 'Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data' (2016) 32 *Computer Law & Security Review* 696–714

Knobel J 'Wrongfulness of trade secret misappropriation; and trade secrets as objects of subjective rights' (2000) *Acta Juridica* 196–212

Kull I 'Withdrawal from the consent to process personal data provided as counter-performance: Contractual consequences' (2020) 13 *Journal of the University of Latvia Law* 33–49

Langa P 'Transformative constitutionalism' (2006) 17 *Stellenbosch Law Review* 351–60

Langhanke C & Schmidt-Kessel M 'Consumer data as consideration' (2015) 4 *Journal of European Consumer and Market Law* 218–23

Laudon K 'Markets and privacy' (1996) 39 *Communications of the ACM* 92–104

UNIVERSITY of the WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

Lazaro C & Le Métayer D 'The control over personal data: True remedy or fairy tale?' (2015) 12 *SCRIPTed* 3–34

Leiner B et al 'A brief history of the Internet' (2009) *ACM SIGCOMM Computer Communication Review* 22–31

Lemley M 'Private property' (2000) 52 *Stanford Law Review* 1545–557

Lerman J 'Big data and its exclusions' (2013) 66 *Stanford Law Review* 55–63

Lessig L 'Privacy as property' (2002) 69 *Social Research* 247–69

Lim H 'The data protection paradigm for the tort of privacy in the age of big data' (2015) 27 *Singapore Academy of Law Journal* 789–821

Lipton J 'Information property rights: Rights and responsibilities' (2004) 56 *Florida Law Review* 135–94

Litman J 'Information privacy/Information property' (2000) 52 *Stanford Law Review* 1283–313

Ludington S 'Reining in the data traders: A tort for the misuse of personal information' (2006) 66 *Maryland Law Review* 140–93

Lynskey O 'Deconstructing data protection in the EU legal order' (2014) 63 *International and Comparative Law Quarterly* 569–97

Mai J 'Big data privacy: The datafication of personal information' (2016) 32 *The Information Society* 192–99

Maple C 'Security and privacy in the Internet of Things' (2017) 2 *Journal of Cyber Policy* 155–84

Marais E 'Expanding the contours of the constitutional property concept' (2016) 2016 *Journal of South African Law* 576–92

Martin N et al 'How data protection regulation affects startup innovation' (2019) 21 *Information Systems Frontiers* 1307–324

Masciandaro A 'Cleaning-up after Carpenter: Personal data as property under the Fourth Amendment' (2021) 51 *Seton Hall Law Review* 1241–277

Mashinini N 'The Processing of personal information using remotely piloted aircraft systems in South Africa' (2020) *De Jure Law Journal* 140–58

McKinstry C 'The HIPAA privacy rule: Flawed privacy exposed when compared with the European Union's General Data Protection Regulation' (2018) *Journal of Health Care Finance* 1–32

McNulty P 'The Public disclosure of private facts: There is life after Florida Star' (2001) 50 *Drake Law Review* 93–158

UNIVERSITY of the
WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

Meacham M 'The perfect storm: How narrowing of the state action doctrine, inconsistency in fourth amendment caselaw, and advancing security technologies converge to erode our privacy rights' (2019) 55 *Idaho Law Revie*w 309–37

Mia N 'The Problems with Prince: A Critical Analysis of Minister of Justice and Constitutional Development v Prince' (2020) 10 *Constitutional Court Review* 401–24

Mittelstadt B 'From individual to group privacy in big data analytics' (2017) 30 *Philosophy & Technology* 475–94

Moosa F 'Understanding the "spirit, purport and objects" of South Africa's Bill of Rights' (2018) 4 *Journal of Forensic, Legal & Investigative Sciences* 1–12

Moosa F 'Is Cryptocurrency "Property" for Tax Administration Purposes?' (2021) 33 *S Afr Mercantile LJ* 364–83

Mostert H 'Engaged citizenship and the enabling state as factors determining the interference parameter of property: A comparison of German and South African law' (2010) 127 *SALJ* 238–73

Mostert M et al 'From privacy to data protection in the EU: Implications for big data health research' (2018) 25 *European Journal of Health Law* 43–55

Mundie C 'Privacy pragmatism: Focus on data use, not data collection' (2014) 93 *Foreign Affairs* 28–38

Mupangavanhu B 'Impact of the Constitution's normative framework on the interpretation of provisions of the Companies Act 71 of 2008' (2019) 22 *PELJ* 1–24

Murphy R 'Property rights in personal information: An economic defense of privacy' (1996) 84 *Georgetown Law Journal* 2381–418

Narayanan A & Shmatikov V 'How to break anonymity of the netflix prize dataset' (2006) *ArXiv* 1–10

Narciso M '"Gratuitous" digital content contracts in EU consumer law' (2017) 6 *Journal of European Consumer and Market Law* 198–206

Naude A & Papadopoulos S 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (1)' (2016) 79 *Journal of Contemporary Roman-Dutch Law* 51–68

Neethling J 'Grondslag vir die erkenning van 'n selfstandige persoonlikheidsreg op privaatheid in die Suid-Afrikaanse reg' (1976) 39 *THRHR* 121–28

Neethling J 'Personality rights: Comparative overview' (2005) 38 *Comparative and International Law Journal of Southern Africa* 210–45

Neethling J 'The Concept of privacy in South African law' (2005) 122 *SALJ* 18–28

Neethling J 'Features of the Protection of Personal Information Bill, 2009 and the law of delict' (2012) 75 *THRHR* 241–55

https://uwcscholar.uwc.ac.za/home

Neethling J ‘Die reg op privaatheid en outonomie Prince v Minister of Justice and Constitutional Development 2017 4 SA 299 (WCC); [2017] 2 All SA 864 (WCC)’ (2018) 15 *LitNet Akademies* 486–95

Nehf J ‘Recognizing the societal value in information privacy’ (2003) 78 *Washington Law Review* 1–92

Nieman A ‘A few South African cents’ worth on bitcoin’ (2015) 18 *PELJ* 1979–2010

Nimmer R & Krauthaus P ‘Information as a commodity: New Imperatives of commercial law’ (1992) 55 *Law and Contemporary Problems* 103–30

Nissenbaum H ‘A contextual approach to privacy online’ (2011) 140 *Daedalus* 32–48

Njotini M ‘Evaluating the position of information or data in the law of property’ (2015) 26 *Stellenbosch Law Review* 220–39

Nolin J ‘Data as oil, infrastructure or asset? Three metaphors of data as economic value’ (2020) 18 *Journal of Information Communication and Ethics in Society* 28–43

Ohm P ‘Broken promises of privacy: Responding to the surprising failure of anonymization’ (2010) 57 *University of California Law Review* 1701–777

Papadopoulos S ‘Revisiting the public disclosure of private facts in cyberworld’ (2009) *Obiter* 30–43

Pappas I et al ‘Big data and business analytics ecosystems: Paving the way towards digital transformation and sustainable societies’ (2018) 16 *Information Systems and e-Business Management* 479–91

Paterson M & McDonagh M ‘Data Protection in an era of big data: The challenges posed by big personal data’ (2018) 44 *Monash University Law Review* 1–31

Pearce H ‘Personality, property and other provocations: exploring the conceptual muddle of data protection rights under EU Law’ (2018) 4 *European Data Protection Law Review* 190–208

Perez C ‘Technological revolutions and techno-economic paradigms’ (2010) 34 *Cambridge Journal of Economics* 185–202

Pistorius T ‘Formation of internet contracts: An analysis of the contractual and security issues’ (1999) 11 *S Afr Mercantile LJ* 282–99

Pittman L ‘The elusive constitutional right to informational privacy’ (2018) 19 *Nevada Law Journal* 135–86

Polykalas S & Prezerakos G ‘When the mobile app is free, the product is your personal data’ (2019) 21 *Digital Policy, Regulation and Governance* 89–101

Pormeister K ‘Informed consent to sensitive personal data processing for the performance of digital consumer contracts on the example of “23andMe’ (2017) 6 *Journal of European Consumer and Market Law* 17–23

https://uwcscholar.uwc.ac.za/home

Posner R ‘The right to privacy’ (1977) 12 *Georgia Law Review* 393–422

Posner R ‘The economics of privacy’ (1981) 71 *The American Economic Review* 405–9

Poullet Y ‘Data protection legislation: What is at stake for our society and democracy?’ (2009) 25 *Computer Law & Security Review* 211–26

Price M ‘Rethinking privacy: Fourth Amendment “papers” and the third-party doctrine’ (2016) 8 J*ournal of National Security Law & Policy* 247–99

Prosser W ‘Privacy’ (1960) 48 *California Law Review* 383–423

Purtova N ‘Property rights in personal data: Learning from the American discourse’ (2009) 25 *Computer Law and Security Review* 507–21

Purtova N ‘Private law solutions in European data protection: Relationship to privacy, and waiver of data protection rights’ (2010) 28 *Netherlands Quarterly of Human Rights* 179–98

Purtova N ‘Property in personal data: A European perspective on instrumentalist theory of propertization’ (2010) 2 *European Journal of Legal Studies* 193–208

Purtova N ‘The illusion of personal data as no one’s property’ (2015) 7 *Law, Innovation, and Technology* 83–111

Purtova N ‘Do property rights in personal data make sense after the big data turn?: individual control and transparency’ (2017) 10 *Journal of Law and Economic Regulation* 64–78

Rabin R ‘Perspectives on privacy, data security, and tort law’ (2017) 66 *DePaul Law Review* 313–38

Radzik L & Schmidtz D ‘Contested commodities’ (1997) 16 *Law and Philosophy* 603–16

Rautenbach I ‘The conduct and interests protected by the right to privacy in section 14 of the Constitution’ (2001) *Journal of South African Law* 115–23

Reding V ‘The European data protection framework for the twenty-first century’ (2012) 2 *International Data Privacy Law* 119–29

Rehman I ‘Facebook-Cambridge Analytica data harvesting: What you need to know’ (2019) *Library Philosophy and Practice* 1–11

Robert R & Smit L ‘The proposal for a directive on digital content: A complex relationship with data protection law’ (2018) 19 *ERA Forum* 159–77

Roederer C ‘Post-matrix legal reasoning: Horizontality and the rule of values in South African law’ (2003) 19 *South African Journal on Human Rights* 57–81

Roos A ‘Core principles of data protection law’ (2006) 39 *The Comparative and International Law Journal of Southern Africa* 102–30

Roos A ‘Data protection: Explaining the international backdrop and evaluating the current South African position’ (2007) 124 *SALJ* 400–37

UNIVERSITY of the
WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

Roos A 'Personal data protection in New Zealand: Lessons for South Africa?' (2008) 11 *PELJ* 60–109

Roos A 'Privacy in the Facebook era: A South African legal perspective' (2012) 129 *SALJ* 375–402

Roos A 'The European Union's General Data Protection Regulation (GDPR) and its implications for South African data privacy law: An evaluation of selected "content principles"' (2020) 53 *Comparative and International Law Journal of Southern Africa* 1–37

Rotenberg M 'Fair information practices and the architecture of privacy (What Larry doesn't get)' (2001) *Stanford Technology Law Review* 1–34

Rubinstein I 'Big data: The end of privacy or a new beginning?' (2013) 3 *International Data Privacy Law* 74–87

Samuelson P 'Privacy as intellectual property?' (1999) 52 *Stanford Law Review* 1125–173

Scholz L 'Privacy as quasi-property' (2016) 101 *Iowa Law Review* 1113–141

Schwartz P 'Privacy and Participation: personal information and public sector regulation in the United States' (1995) 80 *Iowa L Review* 553–618

Schwartz P 'Internet privacy and the state' (1999) 32 *Connecticut Law Review* 815–59

Schwartz P 'Property, privacy and personal data' (2004) 117 *Harvard Law Review* 2055–128

Schwartz P & Peifer K 'Transatlantic data privacy law' (2017) 106 *Georgetown Law Journal* 115–79

Silverio-Fernández M, Renukappa S & Suresh S 'What is a smart device? - A conceptualisation within the paradigm of the Internet of Things' (2018) 6 *Visualization in Engineering* 1–10

Sipior J, Ward B & Volonino L 'Privacy concerns associated with smartphone use' (2014) 13 *Journal of Internet Commerce* 177–93

Solove D 'Privacy and power: Computer databases and metaphors for information privacy' (2001) 53 *Stanford Law Review* 1393–462

Solove D 'Conceptualizing privacy' (2002) 90 *California Law Review* 1087–155

Solove D 'A taxonomy of privacy' (2006) 154 *University of Pennsylvania Law Review* 477–560

Solove D 'A brief history of information privacy law' (2016) *Proskauer on Privacy, PLI* 1–46

Solove D & Hartzog W 'The FTC and the new common law of privacy' (2014) 114 *Columbia Law Review* 583–676

Sono N 'Re-examining the Constitutional Court's approach to the property question since First National Bank of SA Ltd T/A Wesbank v Commissioner, South African Revenue Service; First

https://uwcscholar.uwc.ac.za/home

National Bank of SA Ltd T/A Wesbank v Minister of Finance 2002 4 SA 768 (CC)' (2022) 25 *PELJ* 1–30

Sorieul R, Clift J & Estrella-Faria J 'Establishing a legal framework for electronic commerce: The work of the United Nations Commission on International Trade Law (UNCITRAL)' (2001) 35 *The International Lawyer* 107–22

Stepanov I 'Introducing a property right over data in the EU: The data producer's right – an evaluation' (2019) *International Review of Law, Computers & Technology* 1–22

Strandburg K 'Free fall: The online market's consumer preference disconnect' (2013) 13 *University of Chicago Legal Forum* 95–171

Svantesson D & Clarke R 'Privacy and consumer risks in cloud computing' (2010) 26 *Computer Law and Security Review* 391–97

Swales L 'The Protection of Personal Information Act 4 of 2013 in the context of health research: Enabler of privacy rights or roadblock?' (2022) 25 *PELJ* 1–32

Taylor M 'The EU's human rights obligations in relation to its data protection laws with extraterritorial effect' (2015) 5 *International Data Privacy Law* 246–56

Thaldar D et al 'The multidimensional legal nature of personal genomic sequence data: A South African perspective' (2022) *Frontiers in Genetics* 1–11

Thaldar D & Shozi B 'The legal status of human biological material used for research' (2021) 138 *SALJ* 881–907

Thomas M 'Information as property: Humanism or economic rationalism in the millenium?' (1998) 14 *Queensland University of Technology Law Journal* 203–13

Trakman L, Walters R & Zeller B 'Is privacy and personal data set to become the new intellectual property?' (2019) 50 *International Review of Intellectual Property and Competition Law* 937–70

Tucker C 'The economics of advertising and privacy' (2012) 30 *International Journal of Industrial Organisation* 326–29

Ursic H 'Unfolding the new-born right to data portability: Four gateways to data subject control' (2018) 15 *SCRIPTed* 42–69

Ursic H & Custers B 'Legal barriers and enablers to big data reuse' (2016) 2 *European Data Protection Law Review* 209–21

Van der Bank C 'The right to privacy - South African and comparative perspectives' (2012) 1 *European Journal of Business and Social Sciences* 77–86

Van der Walt A 'Striving for the better interpretation - A critical reflection on the Constitutional Court's Harksen and FNB decisions on the property clause' (2004) 121 *SALJ* 854–78

https://uwcscholar.uwc.ac.za/home

Versaci G 'Personal data and contract law: Challenges and concerns about the economic exploitation of the right to data protection' (2018) 14 *European Review of Contract Law* 374–92

Victor J 'The EU General Data Protection Regulation: Toward a property regime for protecting data privacy' (2013) 123 *The Yale Law Journal* 513–28

Warren S and Brandeis L 'The right to privacy' (1890) 4 *Harvard Law Review* 193–220

White House 'Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy White House report' (2012) 4 *Journal of Privacy and Confidentiality* 95–142

Yakovleva S 'Should fundamental rights to privacy and data protection be a part of the EU's international trade "deals"?' (2018) 17 *World Trade Review* 477–508

Yakowitz J 'Tragedy of the data commons' (2011) 25 *Harvard Journal of Law & Technology* 1–67

Zarsky T 'Desperately seeking solutions: Using implementation-based solutions for the troubles of information privacy in the age of data mining and the internet society' (2004) 56 *Maine Law Review* 13–59

Zarsky T 'Transparent predictions' (2013) 4 *University of Illinois Law Review* 1503–570

Zarsky T 'The privacy-innovation conundrum' (2015) 19 *Lewis & Clark Law Review* 115–68

Zarsky T 'Incompatible: The GDPR in the age of big data' (2017) 47 *Seton Hall Law Review* 995–1020

Zech H 'Information as property' (2015) 6 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 192–97

Zhao B 'The internationalisation of information privacy: Towards a common protection' (2014) 2 *Groningen Journal of International Law* 1–13

Zhu B 'A traditional tort for a modern threat: Applying intrusion upon seclusion to dataveillance observations' (2014) 89 *New York Law Review* 2381–415

Ziegeldorf J, Morchon O & Wehrle K 'Privacy in the Internet of Things: Threats and challenges' (2013) 4 *Security and Communication Networks* 2728–742

Zuiderveen Borgesius F 'Personal data processing for behavioural targeting: Which legal basis?' (2015) 5 *International Data Privacy Law* 163–76

8. REPORTS

American Law Institute *Restatement (Second) of Torts s 652B– s 652E* (1977)

Body of European Regulators for European Communications *BEREC Report on the Data Economy* (2019)

https://uwcscholar.uwc.ac.za/home

Congressional Research Service *Data Protection Law: An Overview* (2019)

Congressional Research Service *Technological Convergence: Regulatory, Digital Privacy, and Data Security Issues* (2019)

Credit Bureau Association *Code of Conduct: Lawful Processing of Personal Information in Credit Sector* (Undated)

EDPS *Meeting the Challenges of Big Data: A Call for Transparency, User Control, Data Protection by Design and Accountability* (2015)

EDPS *Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content* (2017)

EDPS *Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects* (2019)

EDPS *Guidelines 5/2019 on the Criteria of the Right to Be Forgotten in the Search Engines Cases under the GDPR (Part 1)* (2019)

EDPB & EDPS *Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)* (2022)

EC *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards a Thriving Data-Driven Economy* (2014)

EC *How the European Union Works: Your Guide to the EU Institutions* (2014)

EC *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe* (2015)

EC *Impact Assessment: Accompanying the Document Proposals for Directives of the European Parliament and of the Council (1) on Certain Aspects Concerning Contracts for the Supply of Digital Content and (2) on Certain Aspects Concerning Contracts for the Online and Other Distance Sales of Goods* (2015)

EC *Proposal for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content* (2015)

EC *Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World* (2017)

EC *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Building a European Data Economy* (2017)

EC *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European Interoperability Framework - Implementation Strategy* (2017)

https://uwcscholar.uwc.ac.za/home

EC *Impacts of Fully Harmonised Rules on Contracts for the Sales of Goods Supplementing the Impact Assessment Accompanying the Proposal for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Online and Other Distance Sales of Goods* (2017)

EC *Big Data Interoperability Analysis* (2018)

EC *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data* (2020)

EC *European Data Market Study 2021-2023* (2023)

European Court of Human Rights *Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life, Home and Correspondence* (2023)

European Union Agency for Fundamental Rights et al *Handbook on European Data Protection Law* (2018)

European Union Agency for Network and Information Security *Privacy and Data Protection in Mobile Applications - A Study on the App Development Ecosystem and the Technical Implementation of GDPR* (2017)

Executive Office of the President *Big Data and Privacy: A Technological Perspective* (2014)

FTC *Privacy Online: A Report to Congress* (1998)

FTC *Privacy Online: Fair Information Practices in the Electronic Marketplace* (2000)

FTC *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*' (2012)

FTC *Mobile Privacy Disclosures: Building Trust through Transparency*' (2013)

FTC *Cambridge Analytica, LLC: Opinion of the Commission* (2019)

Gellman R *Fair information practices: A basic history* (2019)

Internet Society *Internet Society Policy Brief: IoT Privacy for Policymakers* (2019)

Lenard T & Rubin P *The Big Data Revolution: Privacy Considerations* (2013)

OECD *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980)

OECD *Tracking and Tracing COVID: Protecting Privacy and Data While Using Apps and Biometrics* (2020)

Rosner G & Kenneally E *Privacy and the Internet of Things: Emerging frameworks for policy and design* (2018)

Scassa T *Data Ownership* (2018)

https://uwcscholar.uwc.ac.za/home

SALRC *Project 124: Privacy and Data Protection Report* (2009)

Turow J, Henessy M & Draper N *The tradeoff fallacy - How marketers are misrepresenting American consumers and opening them up to exploitation* (2015)

US Department of Health, Education and Welfare *Records Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (1973)

White House *Big Data: Seizing Opportunities, Preserving Values* (2014)

World Economic Forum *Personal Data: The Emergence of a New Asset Class* (2011)

World Economic Forum *Unlocking the Value of Personal Data: From Collection to Usage* (2013)

World Economic Forum & Kearney A *Rethinking Personal Data: A New Lens for Strengthening Trust* (2014)

WP29 *Opinion 05/2014 on Anonymisation Techniques* (2014)

WP29 *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC* (2014)

WP29 *Guidelines on the Right to Data Portability* (2017)

WP29 *Guidelines on Consent under Regulation 2016/679* (2018)

9. SOUTH AFRICAN STATUTES

UNIVERSITY of the
WESTERN CAPE

Constitution of the Republic of South Africa, 1996

Consumer Protection Act 68 of 2008

Copyright Act 98 of 1978

Electronic Communications and Transactions Act 25 of 2002

National Credit Act 34 of 2005

Protection of Personal Information Act 4 of 2013

10. FOREIGN STATUTES

African Union

African Union Convention on Cyber Security and Personal Data Protection 2014

https://uwcscholar.uwc.ac.za/home

European Union

Charter of Fundamental Rights of the European Union (2000)

Consolidated Version of the Treaty on the Functioning of the European Union 2012

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data 1995

Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services

European Convention on Human Rights 1950

Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Treaty of Lisbon Amending the Treaty on European Union and the Treaty establishing the European Community 2007

Universal Declaration of Human Rights 1948

UNIVERSITY of the
WESTERN CAPE

United States

California Consumer Privacy Act 2018

Constitution of the United States of America 1788

Federal Trade Commission Act 1914

Financial Services Modernization Act 1999

Health Insurance Portability and Accountability Act 1996

Proposed California Consumer Privacy Act Regulations

11. SOUTH AFRICAN CASES

Agri South Africa v Minister for Minerals and Energy 2013 (4) SA 1 (CC)

Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others 2021 (3) SA 246 (CC)

https://uwcscholar.uwc.ac.za/home

Arena Holdings (Pty) Ltd t/a Financial Mail and others v South African Revenue Service and others 2023 (8) BCLR 905 (CC)

Bato Star Fishing (Pty) Ltd v Minister of Environmental Affairs and Others 2004 (4) SA 490 (CC)

Bernstein and Others v Bester and Others 1996 (2) SA 751 (CC)

Bertie Van Zyl (Pty) Ltd and Another v Minister for Safety and Security and Others 2010 (2) SA 181 (CC)

Bester NO and Others v Mirror Trading International (Pty) Ltd t/a MTI (In Liquidation) and Others 2024 (1) SA 112 (WCC)

Carmichele v Minister of State and Security and Another (Centre for Applied Legal Studies Intervening) 2001 (4) SA 938 (CC)

Case and Another v Minister of Safety and Security and Others; Curtis v Minister of Safety and Security and Others 1996 (3) SA 617 (CC)

Chisuse and Others v Director-General, Department of Home Affairs and Another 2020 (6) SA 14 (CC)

Cool Ideas 1186 CC v Hubbard 2014 (4) SA 474 (CC)

Dawood and Another v Minister of Home Affairs and Others; Shalabi and Another v Minister of Home Affairs and Others; Thomas and Another v Minister of Home Affairs and Others 2000 (3) SA 936 (CC)

Department of Land Affairs and Others v Goedgelegen Tropical Fruits 2007 (6) SA 199 (CC)

Discovery Ltd and Others v Liberty Group Ltd 2020 (4) SA 160 (GJ)

Du Plessis and Others v De Klerk and Another 1996 (3) SA 850 (CC)

Dun and Bradstreet (Pty) Ltd v SA Merchants Combined Credit Bureau (Cape) (Pty) Ltd 1968 (1) SA 209 (C)

Ex Parte Chairperson of the Constitutional Assembly: In Re Certification of the Constitution of the Republic of South Africa, 1996 1996 (4) SA 744 (CC)

Financial Mail (Pty) Ltd and Others v Sage Holdings Ltd and Another 1993 (2) SA 451 (A)

First National Bank of SA Ltd t/a Wesbank v Commissioner; South African Revenue Service; First National Bank of SA Ltd t/a Wesbank v Minister of Finance 2002 (4) SA 768 (CC)

Gaertner and Others v Minister of Finance and Others 2014 (1) SA 442 (CC)

Harchris Heat Treatment (Pty) Ltd v Iscor 1983 (1) SA 548 (T)

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd and Others: In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others 2001 (1) SA 545 (CC)

UNIVERSITY of the WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

Khumalo and Others v Holomisa 2002 (5) SA 401 (CC)

Klaase and Another v Van Der Merwe NO and Others 2016 (6) SA 131 (CC)

Kumalo v Cycle Lab (Pty) Ltd (2011) JOL 27372 (GSJ)

Laugh It Off Promotions CC v SAB International (Finances) BV 2006 (6) SA 144 (CC)

Law Society of South Africa and Others v Minister of Transport and Another 2011 (1) SA 400 (CC)

Mighty Solutions t/a Orlando Service Station V Engen Petroleum Ltd And Another 2016 (1) SA 621 (CC)

Minister of Health and Another v New Clicks South Africa (Pty) Ltd and Others 2006 (2) SA 311 (CC)

Minister of Justice and Constitutional Development and Others v Prince and Others 2018 (6) SA 393 (CC)

Mistry v Interim Medical and Dental Council of South Africa and Others 1998 (4) SA 1127 (CC)

Mkontwana v Nelson Mandela Metropolitan Municipality; Bissett v Buffalo City Municipality; Transfer Rights Action Campaign v MEC, Local Government and Housing, Gauteng 2005 (1) SA 530 (CC)

Mphela and Others v Haakdoornbult Boerdery CC and Others 2008 (4) SA 488 (CC)

My Vote Counts v Speaker of the National Assembly and Others 2016 (1) SA 132 (CC)

Natal Joint Municipal Pension Fund v Endumeni Municipality 2012 (4) SA 593 (CC)

National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others 1999 (1) SA 6 (CC)

National Credit Regulator v Opperman 2013 (2) SA 1 (CC)

National Media Ltd and Another v Jooste 1996 (3) SA 262 (A)

NM and Others v Smith and Others (Freedom of Expression Institute as Amicus Curiae) 2007 (5) SA 250 (CC)

O' Keeffe v Argus Printing and Publishing Co Ltd 1954 (3) SA 244 (C)

Pharmaceutical Manufacturers Association of SA & Another: In re Ex Parte President of the Republic of South Africa and Others 2000 (2) SA 674 (CC)

Phumelela Gaming and Leisure Ltd v Grundlingh 2007 (6) SA 350 (CC)

S v Makwanyane and Another 1995 (3) SA 391 (CC)

S v Zuma and Others 1995 (2) SA 642 (CC)

UNIVERSITY of the WESTERN CAPE

https://uwcscholar.uwc.ac.za/home

Shoprite Checkers (Pty) Ltd v MEC for Economic Development, Environmental Affairs and Tourism, Eastern Cape 2015 (6) SA 125 (CC)

University of Johannesburg v Auckland Park Theological Seminary and Another 2021 (6) SA 1 (CC)

Waste-tech (Pty) Ltd v Wade Refuse (Pty) Ltd 1993 (3) All SA 542 (W)

12. FOREIGN CASES

Canada

R v Stewart (1988) 1 SCR 963 (SCC)

European Union

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado (2011) Joined Cases C-468/10 and C-469/10 ECLI:EU:C:2011:777

Google Spain v AEPD & Mario Costej Case C-131/12 ECLI:EU:C:2014:317

Joined Cases C-293/12 and C-594/12 Digital Rights Ireland v Minister for Communications, Marine and Natural Resources, Seitlinger and Others (2014) ECLI:EU:C:2014:238

Maximilian Schrems v Facebook Ireland Limited (2021) 6 Ob 56/21k (Oberster Gerichtshof)

Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme' Case C-13/16 ECLI:EU:C:2017:336

Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen Joined Cases C 92/09 and C 93/09 ECLI:EU:C:2010:662

United Kingdom

Boardman and Another v Phipps (1967) 2 46 (AC)

Fairstar Heavy Transport NV v Philip Jeffrey Adkins, Claranet Limited (2013) Civ 886 (EWCA)

Oxford v Moss (1979) 68 183 (Cr App R)

Regina (Veolia ES Nottinghamshire Ltd) v Nottinghamshire County Council [2010] Civ 1214 (EWCA)

https://uwcscholar.uwc.ac.za/home

United States

Cline v Rogers (1996) 87 F3d 176 (6th Cir)

Deshaney v Winnebago County Department of Social Services (1989) 489 US 189

Dobbs v Jackson Women's Health Organization (2022) 142 SCt 2228

Doe v Borough of Barrington (1990) 729 F Supp 376 (DNJ)

Dwyer v American Express Co (1995) 652 NE 2d 1351 (Ill App Ct)

Florida Star v BJF (1989) 491 US 524

Fraley v Facebook, Inc (2011) 830 F Supp 2d 785 (NC Cal)

Griswold v Connecticut (1965) 381 US 479

Howard v Aspen Way Enterprises, Inc (2017) 406 P3d 1271 (Wyo)

J P v DeSanti (1981) 653 F2d 1080 (6th Cir)

Kallstrom v City of Columbus (1998) 136 F3d 1055 (6th Cir)

Katz v United States (1967) 389 US 347

McElhaney v Thomas (2017) 405 P3d 1214 (Kan)

Meyer v Nebraska (1923) 262 US 390

National Aeronautics and Space Administration v Nelson (2011) 131 SCt 746

Nixon v Administrator of General Services (1977) 433 (US) 425

Olmstead v United States (1928) 277 US 438

Pierce v Society of Sisters (1925) 268 US 510

Planned Parenthood of Southeastern Pennsylvania et al v Casey, Governor of Pennsylvania et al (1992) 505 US 833

Remsburg v Docusearch, Inc (2003) 816 A 2d 1001 (NH)

Roe v Wade (1973) 410 US 113

Rojas-Lozano v Google, Inc (2016) 159 F Supp 3d 1101 (ND Cal)

Russel v Gregoire (1997) 124 F3d 1079 (9th Cir)

Shibley v Time Inc (1975) 341 NE 2d 337 (Ohio Ct App)

Snyder v Phelps (2011) 562 US 443

Sorrell v IMS Health Inc (2011) 564 (US) 552

https://uwcscholar.uwc.ac.za/home

United States v Westinghouse Electric Corporation (1980) 638 F2d 570 (3d Cir)

Washington v Glucksberg (1997) 521 US 702

Whalen v Roe (1977) 429 (US) 589

13. PATENTS

Spiegel J et al 'Method and system for anticipatory package shipping' US Patent US8615473B2 issued on 24 December 2013 available at *https://patents.google.com/patent/US8615473B2/en* (accessed 25 February 2021)

14. SPEECHES

Reding V 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age' 2012 available at *http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm* (accessed 4 May 2024)

Vestager M 'Making Data Work for Us' 2016 available at *http://web.archive.org/web/20161015230600/http:/ec.europa.eu/commission/2014-2019/vestager/announcements/making-data-work-us_en* (accessed 4 May 2024)

UNIVERSITY of the
WESTERN CAPE

https://uwcscholar.uwc.ac.za/home