UNIVERSITY OF KWAZULU-NATAL

COLLEGE OF LAW AND MANAGEMENT STUDIES

HOW WILL THE INFORMATION REGULATOR MANAGE AND CONTROL ADVANCEMENTS IN TECHNOLOGY TO MINIMISE ITS ADVERSE EFFECTS ON THE PROTECTION OF PERSONAL INFORMATION?

A DISSERTATION PRESENTED

BY

SARIKA RAMCHARAN

TO

THE COLLEGE OF LAW AND MANAGEMENT STUDIES

SCHOOL OF LAW

IN PARTIAL FULFILMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF LAWS (LLM)

IN

BUSINESS LAW

Supervisor: Dr Lee Swales

TABLE OF CONTENTS

DECLARATION 4
ACKNOWLEDGEMENTS 5
LIST OF ACRONYMS AND ABBREVIATIONS 6
CHAPTER 1: RESEARCH OVERVIEW 7
1.1. INTRODUCTION 7
1.2. BACKGROUND 10
1.3. STATEMENT OF PURPOSE 13
1.4. RATIONALE 13
1.5. RESEARCH QUESTIONS 14
1.6. THEORETICAL FRAMEWORK 14
1.7. RESEARCH METHODOLOGY 15
2.1 INTRODUCTION 16
2.2 SOUTH AFRICAN COMMON LAW 17
2.2.1 Privacy Protection 17
2.2.2 Remedies for Privacy Infringements 18
2.3 CONSTITUTIONAL PROTECTION 20
2.4 STATUTORY DATA PROTECTION 21
2.4.1 Sectoral-specific legislation 21
2.4.2 Specific Data Protection: The POPIA 22
2.5 CONCLUDING REMARKS 29
CHAPTER 3: AN EVALUATION OF THE POPIA ENFORCEMENT MECHANISMS AND PENALTY REGIME TO ADDRESS TECHNOLOGICAL ADVANCEMENTS 31
3.1 INTRODUCTION 31
3.2 OVERSIGHT AND ENFORCEMENT STRUCTURE 31
3.3 ENFORCEMENT MECHANISMS 32
3.3.1 Complaints 33
3.3.2 Warrants for search and seizure 34
3.3.3 Assessment 35
3.3.4 Enforcement Committee and Enforcement Notices 35
3.3.5 Civil Remedies 36
3.4 PENALTY REGIME 36
3.4.1 Offences and Penalties 36
3.4.2 Administrative Penalties 37
3.5 CONCLUDING REMARKS 38
4.1 INTRODUCTION 39
4.2 FUNCTIONS OF THE INFORMATION REGULATOR 39

4.2.1. The Regulation of Technology-Specific or Technologically Neutral Data Protection 42
4.3 TECHNOLOGY FORESIGHT ACTIVITIES OF DPAs: LESSONS FROM THE UNITED KINGDOM AND NEW ZEALAND 44
4.3.1 Overview 44
4.3.2 New Zealand 44
4.3.3 United Kingdom 47
4.4 CONCLUDING REMARKS 51
CHAPTER 5: DATA PROTECTION LAW REFORM IN THE EUROPEAN UNION, UNITED KINGDOM AND NEW ZEALAND 53
5.1 INTRODUCTION 53
5.2 REFORM OF THE EU DATA PROTECTION REGIME 53
5.2.1 Background 53
5.2.2 Changes to the EU Data Protection Regime 55
5.3 UNITED KINGDOM 62
5.3.1 Background 62
5.3.2 The UK Data Protection Regime 63
5.4 NEW ZEALAND 65
5.4.1 An Overview of Statutory Data Protection in New Zealand 65
5.4.2 Reform of the Statutory Data Protection Regime 66
5.5 CONCLUDING REMARKS 69
6.1 OVERVIEW 70
6.2 CONCLUSION 70
6.3.1 Recommendations for Technological Foresight 72
6.3.2 Recommendations for Reform 73
7. BIBLIOGRAPHY 75

DECLARATION

I, Sarika Ramcharan, student number: 200104529, hereby declare that this dissertation is my own unaided work and has not been submitted to any other university.

I have thoroughly cited and acknowledged all the sources of my research.

Sramcharan

……

Sarika Ramcharan

200104529

ACKNOWLEDGEMENTS

I acknowledge the following people who supported me throughout this academic journey:

To my amazing family, thank you for sacrificing the countless hours we usually spend as family time for me to focus on my dissertation.

To my employer, Transnet SOC Limited, my sincere gratitude for providing me with a bursary to pursue my LLM qualification.

To my supervisor, Dr Lee Swales, for your valuable and meaningful academic guidance.

Lastly, to my manager, Marissa Damons, thank you for your encouragement and never hesitating to give me time off from work to pursue my research.

LIST OF ACRONYMS AND ABBREVIATIONS

4IR	Fourth Industrial Revolution
DPAs	Data Protection Authorities
DPIA	Data Protection Impact Assessment
EC	European Commission
ECTA	Electronic Communications and Transactions Act No. 25 of 2002
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
NCA	National Credit Act
NZ	New Zealand
OECD	Organisation for Economic Cooperation and Development
PAIA	Promotion of Access to Information Act
PETs	Privacy Enhancing Technologies
POPIA	The Protection of Personal Information Act
SA	The Republic of South Africa
SALRC	South African Law Reform Commission
UK	United Kingdom

CHAPTER 1: RESEARCH OVERVIEW

1.1. INTRODUCTION

"Personal data is the new oil of the internet and the new currency of the digital world"[1]

The proliferation of computer systems and Information and Communications Technology (ICT) from the 1970s prompted law makers around the world to begin developing data protection laws to protect personal information or data[2] and the right to privacy.[3] Data protection laws have a uniform objective to regulate the processing of personal information or data[4] and are designed to afford safeguards whenever ICT is used to process personal information.[5]

A substantial portion of global trade is centred around the use of personal data, which is regarded as the 'new oil' of online activity by virtue of the large volumes of personal information processed across the world[6] due to rapid developments in information technology.[7] This resulted in heightened interest in data privacy[8] and data protection and the

---

[1] M Kuneva 'Keynote Speech SPEECH/09/156' (Roundtable on Online Data Collection, Targeting and Profiling)' available *at http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm, accessed on 30 March 2019.*

[2] The terms 'personal information' and 'personal data' are used synonymously throughout this dissertation. 'Personal information' is defined in section 1 of the POPIA. See further article by A Roos 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position' (2007) 124(2) *SALJ* 401, where she draws a distinction between these two terms. She explains that 'data' is defined as "unstructured facts or raw material that needs to be processed and organized to produce information," whereas 'information' refers to "data that are organized, structured and meaningful to the recipient position."

[3] Ibid at 403. The Federal State of Hesse in Germany passed the first data protection law in 1970, followed by national laws in several other states such as Sweden (1973), the United States (1974), Germany (1977) and France (1978).

[4] A Roos 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position' (note 2 above) 402.

[5] P Hustnix 'EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection' in Cremona M et al (ed) *New Technologies and EU Law* 1ed Oxford (2017) 123-172.

[6] This phenomenon is often referred to as transborder data flows. See A Roos 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position' (note 2 above) 403.

[7] United Nations Conference on Trade and Development 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' available at *https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_summary_en.pdf,* accessed on 10 April 2019.

[8] The terms 'data protection and 'data privacy' are used synonymously throughout this dissertation. See Chapter 2, paragraph 2.1 for a discussion on these terms. See also A Roos 'Data Privacy Law' in D Van der Merwe, A Roos, T Pistorius, S Eiselen and S Nel (eds) *Information and Communications Technology Law* 2ed 2016 368, where it is explained that "[D]ata privacy law can thus be defined as a set of measures aimed at safeguarding data subjects from harm resulting from the computerised or manual processing of their personal information by data controllers."

development of three key international instruments.[9] The effects of technological advancements on data privacy raise various concerns.[10] It is likely that by the end of 2020, 50 billion devices will have wireless connection to the internet.[11] In light of rapid technological developments, there has been a boom in data protection regulation with 126 countries having enacted data protection laws as at June 2018.[12]

In South Africa (SA), the right to privacy is protected by the common law[13] and is entrenched as a fundamental human right in terms of the Constitution.[14] The South African government realised that current protection was not adequate, and acknowledged the need for specific data protection legislation to address the surveillance potential of modern computerised systems and databases.[15] In order to bring SA on par with its international counterparts, in 2005, the South African Law Reform Commission (SALRC) was mandated to investigate data privacy in instances where personal data is processed by the State or other persons and to recommend legislative steps which should be taken in this regard.[16]

Although SA was slow to introduce data protection legislation, an advantage is that it is able to learn from and reflect on legislation adopted by other jurisdictions.[17] Burchell correctly predicted that the country's data protection legislation would be aligned to the

---

[9] The first two international instruments that were enacted in 1980 are the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. The third international instrument that aims to protect personal data is the EU Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data which was passed in 1995.

[10] "The emergence of new, evolving and emerging computer and ICT have fuelled data privacy concerns due to the size and amount of data that can be collected, the speed of such collection, improved storage capacities, increased potential of manipulation of personal data as well as the ease with which personal information can be shared across the globe and social media." See AB Makulilo *African Data Privacy Laws* in Law, Governance and Technology Series 1ed (2017) 3.

11 World Economic Forum 'Data Policy in the Fourth Industrial Revolution: Insights on personal data' available at *https://www.weforum.org/whitepapers/data-policy-in-the-fourth-industrial-revolution-insights-on-personal-data,* accessed on 01 April 2019.

*12*Global Convergence of Data Privacy Standards and Laws: 'Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi' available at *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3184548,* accessed on 10 April 2019.

[13] At common law, the delictual protection of the right to privacy enjoys recognition as an independent right of personality. Refer to Chapter 2 for a detailed discussion on the data protection regime in SA.

[14] Section 14 (d) of the Constitution of the Republic of South Africa Act No. 108 of 1996 (hereinafter referred to as "the Constitution") (which took effect on 4 February 1997) provides that "Everyone has the right to privacy, which includes… the right not to have the privacy of their communications infringed."

[15] South African Law Reform Commission Discussion Paper 109 (Project 124) 'Privacy and Data protection' (2005) iv available at *https://www.justice.gov.za/salrc/dpapers/dp109.pdf,* accessed on 04 June 2019.

[16] Ibid at 13.

[17] J Burchell 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid' (2009) 13.1 *EJCL* 11.

Organisation for Economic Cooperation and Development (OECD) guidelines.[18] In 2009, the SALRC published a final report, entitled "Privacy and Data Protection Project 124 Report" ("SALRC Final Report").[19] It recommended that specific data protection legislation be enacted in the form of the Protection of Personal Information Bill B 9D – 2009 which contained eight principles aligned to the OECD guidelines.

The much-awaited Protection of Personal Information Act No. 4 of 2013 (POPIA) was signed into law on 19 November 2013.[20] Its overall objective is to give effect to the constitutional right to privacy. The purpose of the POPIA is to *inter alia*, safeguard the processing[21] of personal information[22] by public and private bodies and to provide for an Information Regulator to exercise certain powers and functions in terms of the POPIA and the Promotion of Access to Information Act 2 of 2000.[23] However, to date, not all the POPIA provisions have come into effect.[24] The surge in data growth since the partial promulgation of the POPIA prompted the Information Regulator to request that the President bring the remaining provisions of this Act into force and effect from 1 April 2020.[25]

Effective enforcement of the POPIA depends on the Information Regulator being fully operational to actively carry out its mandate when the remaining provisions of the Act come into force and effect.[26] The Information Regulator was appointed by the National Assembly on 09 September 2016, as a juristic person to serve as the core supervisory body mandated to ensure compliance with the POPIA and the law in general, in so far as protecting

---

[18] Ibid at 14-15.

19 The South African Law Reform Commission Project 124 'Privacy and Data Protection Report' dated 2009 available at *https://www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf,* accessed on 15 June 2019.

[20] No. 4 of 2013 published in GN 912 in GG 37067 of 26 November 2013.

[21] The term 'processing' is defined in Section 1 of the POPIA.

[22] See section 1 of the POPIA for the definition of 'personal information', which is broadly defined to include various categories of personal information relating to an identifiable living natural person and an existing juristic person. Note further that the POPIA defines a "person" in section 1 to include reference to both natural persons or juristic persons.

[23] Section 2 of the POPIA sets out its purpose.

[24] A proclamation published on 11 April 2014 declared that certain sections of the POPIA will become effectual as at the date of such publication, namely, section 1 (definitions); Part A of Chapter 5 (establishment, duties and powers of the Information Regulator) and sections 112 and 113 (empowering provisions for the Minister of Justice and Constitutional Development to issue regulations and the procedure to be followed thereto).

25 'The waiting game is over for PoPI Act' *IOL* 17 February 2020 available at *https://www.iol.co.za/business-report/economy/the-waiting-game-is-over-for-popi-act-42881708, accessed* on 03 March 2020.

[26] Section 114 (1) of the POPIA contains transitional arrangements where persons (private and public) undertaking all forms of processing of personal information are required to comply with the POPIA within one year after its commencement.

personal data is concerned. [27] The Information Regulator is granted extensive powers and functions to ensure that personal data is processed lawfully by applying the principles set down in the POPIA.[28] The body is made up of a chairperson and four individuals as ordinary members.[29]

To ensure effective implementation of the POPIA, the Information Regulator published Regulations[30] ("POPIA Regulations") on 08 September 2017. These are mostly procedural in nature, but, it is noteworthy that an Information Officer[31] appointed by a public or private body is required to conduct a personal information impact assessment with adequate measures and standards to drive compliance with the lawful processing conditions.[32]

1.2. BACKGROUND

Data privacy has always centred around the evolution of technologies and data protection laws consequently establish data protection authorities (DPAs).[33] DPAs[34] are referred to by different names in foreign jurisdictions, including Regulator,[35] Office of the Commissioner,[36] Inspectorate,[37] Directorate,[38] Authority[39] and Supervisor.[40]

---

[27] The Information Regulator is established in terms of section 39 of the POPIA.

[28] The scope of the Information Regulator's duties, powers and functions are fully set out in section 40 of the POPIA.

[29] Section 41(1)(a) (i) and (ii) sets out the composition and eligibility criteria for members appointed by the Information Regulator who must be suitably qualified, fit and proper. At least one of the members must be a practising attorney or a professor of law at a university and the remainder of the members must be appointed taking into account their qualifications, experience and expertise relating to the objectives of the Information Regulator. This section further sets out the term of appointment of the Chairperson and other members of the Information Regulator.

[30] Regulations relating to the Protection of Personal Information, 2017, published in accordance with section 112(2) of the POPIA - GN R 2017 in *GG* 41105 (not yet proclaimed).

[31] An 'Information Officer' is specifically defined in section 1 of the POPIA.

[32] Regulation 4(1)(b) of the POPIA Regulations.

33 European Data Protection Supervisor 'Technology Monitoring' available at *https://edps.europa.eu/data-protection/our-work/technology-monitoring_en*, *accessed* on 13 April 2019.

[34] This dissertation uses the term 'DPAs' to refer to foreign data protection regulators.

[35] The POPIA uses the term "Information Regulator" and as such this dissertation uses this term in discussions on South African law and the POPIA.

36 The DPA in Australia is referred to as the Office of the Australian Information Commissioner and in Canada the DPA is referred to as the Office of the Privacy Commissioner of Canada.

[37] The DPA in Estonia is referred to as the Estonian Data Protection Inspectorate.

[38] The DPA in Argentina is referred to as the National Directorate for Personal Data Protection.

[39] The DPA in Belgium is referred to as the Data Protection Authority and in Hungary the DPA is referred to as the National Authority for Data Protection and Freedom of Information.

[40] The European Data Protection Supervisor is the European Union's independent data protection authority.

In the wake of the Fourth Industrial Revolution (4IR),[41] new digital technologies have the ability to process an exorbitant amount of personal data on a daily basis.[42] By their very nature, digital technologies have revolutionised the ability to copy, interlink, compare, combine and collect an enormous amount of personal data without a data subject's[43] consent, thereby directly contributing to loss of control over his or her data privacy.[44] Automatic processing of personal data using technologies increases the chances of intercepting, sharing, storing, accessing and selecting such information.[45] Certain personal information is collected "surreptitiously by technological inventions" without the knowledge of the data subject.[46]

New wireless technology such as mobile communication networks which enable geographic location of mobile devices can also intrude on privacy if used as location-based advertising. The latest technologies such as cloud computing[47] and big data[48] pose bigger challenges to data privacy. Individuals do not have control of their personal information in the cloud, which can be stored on various servers anywhere in the world. The manner of the processing, the place at which processing occurs and the identity of the party undertaking such processing are thus unknown. Big data is regarded as contrary to data privacy principles because data collected for a specific purpose is processed for an unrelated purpose without

---

41 The 4IR can be described as "the advent of 'cyber-physical systems' involving entirely new capabilities for people and machines which represents entirely new ways in which technology becomes embedded within societies and even our human bodies". Examples include genome editing, new forms of machine intelligence, breakthrough materials and approaches to governance that rely on cryptographic methods such as the blockchain. See World Economic Forum 'What is the Fourth Industrial Revolution?' available at *https://www.weforum.org/agenda/2016/01/what-is-the-fourth-industrial-revolution/*, accessed on 10 April 2019.

42 ISACA 'Enforcing Data Privacy in the Digital World' available *http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Enforcing-Data-Privacy-in-the-New-Digital-World.aspx*, accessed on 13 April 2019.

[43] Section 1 of the POPIA defines a "data subject" as "a person to whom the personal information relates."

44 J Van den Hoven et al 'Privacy and Information Technology' (2018) *The Stanford Encyclopedia of Philosophy* 3 available at *https://plato.stanford.edu/archives/sum2018/entries/it-privacy/*, accessed on 16 April 2019.

[45] D Van der Merwe et al *Information Communications Technology* Law 2ed (2016) 365.

[46] Examples of technological inventions include cookies, radio frequency identification, and the use of scanners on mobile devices where Wi-Fi or Blue Tooth is activated to collect personal data. See D Van der Merwe et al *Information Communications Technology Law* (note 45 above) 365.

47 Cloud computing is defined as "a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using internet technologies." See Gartner Glossary available at *https://www.gartner.com/en/information-technology/glossary/cloud-computing*, accessed on 11 July 2019. See further D Van der Merwe et al *Information Communications Technology Law* (note 45 above) 366, where the author explains that "a cloud computing service provider can offer various services such as data storage space as well as software applications to multiple customers on demand. In other words, instead of storing data and software on a user's hard drive, it is now stored on various servers which could be located anywhere in the world and accessed, when needed, via the Internet."

[48] Big Data is defined as "the creation and analysis of massive data sets. Data collected in one area can be linked to data collected in other areas and the data can then be analysed to produce new inferences." For example, data is collected from multiple sources such as mobile banking transactions, Tweets, satellite images, online searches

the consent of the person to whom the personal data relates.[49] Furthermore, the Internet of Things[50] creates risks associated with poor security measures, exposing the data subject to data losses, unlawful or unauthorised access to personal information, unlawful surveillance, and infection by malware.[51]

With technology constantly evolving, data protection laws will need to keep pace to ensure that legal protection of data privacy remains adequate for DPAs to meaningfully enforce compliance. The focus of this research is therefore limited to sections 40(1) (b)(ii)[52] and 40(e)(i) and (ii)[53] of the POPIA, which broadly encompass the specific duties, functions and powers of the Information Regulator to research and monitor developments in technology, undertake research, and propose to Parliament that SA accepts any international instrument, or makes necessary legislative amendments aimed at protecting personal information. These powers and functions are important in ensuring that the Information Regulator is proactive in facilitating improved regulatory protection of personal information by addressing the data privacy challenges posed by new or emerging technologies.

Against this background, this research addresses how the Information Regulator will execute its mandate to manage and control advancements in technology to minimise its adverse effects on data protection. Accordingly, it explores the regulation of data protection in SA, data protection laws adopted in foreign jurisdictions, and academic discourses and case law. Given that the POPIA is a new piece of legislation, an interesting feature of this

---

and online purchase information. See D Van der Merwe et al *Information Communications Technology Law* (note 45 above) 366.

[49] Ibid at 367.

[50] The Internet of Things is defined as "an infrastructure in which billions of sensors embedded in common, everyday devices – 'things' as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities." These everyday devices include, amongst others, television, exercise equipment and appliances. See the European Union's Article 29 Data Protection Working Party 'Opinion 8/2014 on Recent Developments on the Internet of Things' WP 223 (2014) available at *https://www.dataprotection.ro/servlet/ViewDocument?id=1088*, accessed on 20 July 2019. See further D Van der Merwe et al *Information Communications Technology Law* (note 45 above) 368.

[51] D Van der Merwe et al *Information Communications Technology Law* (note 45 above) 368.

[52] Section 40(1)(b)(ii) of the POPIA encompasses the Information Regulator's mandate to "monitor and enforce compliance by undertaking research into, and monitoring developments in, information processing and computer technology to ensure that any adverse effects of such developments on the protection of the personal information of data subjects are minimised, and reporting to the Minister the results of such research and monitoring."

[53] Section 40(e)(i) and (ii) of the POPIA deals specifically with the Information Regulator's duty to "conduct research and to report to Parliament, from time to time on the desirability of the acceptance, by South Africa, of any international instrument relating to the protection of the personal information of a data subject;" and "on any other matter, including necessary legislative amendments, relating to protection of personal information that, in the Regulator's opinion, should be drawn to Parliament's attention."

research is to investigate the approach followed by foreign jurisdictions to address new data privacy challenges posed by technological developments.

1.3. STATEMENT OF PURPOSE

This dissertation assesses and evaluates the manner in which the Information Regulator will discharge its powers, duties and functions in terms of section 40(1)(b)(ii) of the POPIA. It examines the data protection legal regimes in SA and foreign jurisdictions such as the European Union (EU), United Kingdom (UK) and New Zealand (NZ) in order to determine if amendments are required to the POPIA, which the Information Regulator is mandated to consider in line with section 40(e) of this Act.

Overall, this dissertation assesses whether, in its current form, the POPIA is adequate to manage and control the adverse effects of technological advancements as well as the role of the Information Regulator to monitor and enforce compliance in this regard. Based on an analysis of developments in foreign data protection regimes, it also proposes recommendations for consideration by the Information Regulator to bring the POPIA Act in line with such developments.

1.4. RATIONALE

Technology is evolving at a rapid pace in the era of the 4IR. In order to remain effective and adequate, the data protection regulatory landscape will need to be reviewed and updated. The POPIA's key purpose is to uphold the constitutional right to privacy by ensuring that, notwithstanding advancements in technology, data privacy is not sacrificed. The Information Regulator is therefore empowered to prevent technological developments from impairing the right to privacy. In anticipation of the Information Regulator being robust in executing its mandate in terms of the POPIA, scholarly research and dialogue has occurred in SA on *inter alia*, the level of compliance required in terms of the POPIA to avoid the consequences of non-compliance. However, limited scholarly research or dialogue has focused specifically on the Information Regulator's mandate in terms of Sections 40(1)(b)(ii) and 40(e) of the POPIA.

The practical application and enforcement of the POPIA is currently not known. This dissertation thus aims to contribute to the debate on the Information Regulator's mandate to

conduct research into and monitor developments in technology by examining developments in foreign jurisdictions which address the data privacy challenges associated with the evolving technological landscape.

1.5. RESEARCH QUESTIONS

1.5.1 How does South African law regulate data protection to safeguard the right to privacy? Is the regulatory landscape effective in the era of constant technological developments to adequately protect a data subject's right to privacy?

1.5.2 Does the POPIA contain adequate provisions and enforcement mechanisms to guard against the adverse effects of new technologies used to process personal information? Is the current penalty regime provided for in the POPIA effective in this regard?

1.5.3 What are the regulatory powers, duties and functions of the Information Regulator in terms of the POPIA to ensure that the protection of personal information is minimally affected by technological developments?

1.5.4 In comparison to South African law, what are the obligations of foreign data protection regulators to monitor and address challenges to data protection associated with advancements in technology? Are there any new developments in foreign data protection law to minimise the challenges posed by new technologies?

1.5.5 How can the Information Regulator afford better protection and enforce compliance in response to technological developments? Can this be achieved by enhancing the current regulatory landscape to pre-empt and mitigate the adverse effects new technologies will have on the protection of personal information in South Africa?

1.6. THEORETICAL FRAMEWORK

Taking into account the research topic, the research questions, the literature reviewed and the data collection methodology, this research adopts the positivist approach to assess the challenges new technologies pose to the protection of personal information. This approach is favoured because the underlying research is procedural in nature and as such focusses on the

principles formulated under South African and foreign law. The dissertation focusses on the written law as it is, without reliance on the morality of the actions taken by countries.

1.7. RESEARCH METHODOLOGY

A desktop based research method was employed to review legislation, case law, journal articles and other academic sources relevant to data protection. Both primary and secondary sources of data housed in libraries and via electronic sources were consulted. Substantial emphasis was placed on foreign data protection legal regimes.

CHAPTER 2: THE SOUTH AFRICAN DATA PROTECTION REGIME

2.1 INTRODUCTION

In SA, the right to privacy is protected by the Constitution as a fundamental human right,[54] as well as by the common law and the POPIA,[55] which, once in full effect, will provide an omnibus form of data protection.[56] The Constitutional Court described the right to privacy as "the right to be left alone."[57] In particular, the South African courts[58] have accepted the definition of privacy coined by Neethling, which provides as follows:

> Privacy is an individual condition of life characterised by exclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has determined himself to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private.[59]

This definition suggests that privacy rights extend to data privacy,[60] where an individual should be able to control his or her personal data by conducting personal affairs without any unlawful interference.[61] Bygrave is of the view that data privacy touches on more than general privacy concerns.[62]

The Constitutional Court[63] expanded the right to privacy to information (data) privacy by strongly asserting that the right to privacy is not only in relation to an individual's intimate

---

[54] Section 14 of the Constitution.

[55] The POPIA is not yet in full force and effect. See discussion under Chapter 1, paragraph 1.1 above.

[56] A Roos 'Data Protection Law in South Africa' in AB Makulilo *African Data Privacy Laws*: Springer (2017) 194.

[57] *NM and Others v Smith and Others (Freedom of Expression Institute as Amicus Curiae)* 2007 (7) BCLR 751 (CC) 32; *Minister of Justice and Constitutional Development and Others v Prince (Clarke and Others Intervening); National Director of Public Prosecutions and Others v Acton* (CCT108/17) [2018] ZACC 30; 2018 (10) BCLR 1220 (CC); 2018 (6) SA 393 (CC); 2019 (1) SACR 14 (CC) where Zondo ACJ confirmed that the "right to privacy is a right to be left alone."

[58] *Jooste v National Media Ltd* 1994 (2) SA 634 (C) at 645; *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 (4) SA 376 (T) at 384; *Bernstein v Bester NO* 1996 (2) SA 751 (CC) at 789; *Swanepoel v Minister van Veiligheid en Sekuriteit* 1999 (4) SA 549 (T) at 553.

[59] J Neethling *Die Reg op Privaatheid* (LLD thesis Unisa 1976) 287; J Neethling et al *Neethling's Law of Personality* 2 ed (2005) 32.

[60] The term 'data privacy' does not feature in any case law or adopted data protection legal instrument but it has been commonly used in the academic literature, mainly to single out the critical issue at stake emanating from the risks posed by technologies.

[61] J Neethling *Die Reg op Privaatheid* (LLD thesis Unisa 1976) (note 59 above) at 1.2.1.

[62] LA Bygrave *Data Privacy Law: An International Perspective* (2014) 3. See also A Roos 'Data Privacy Law' (note 8 above) 367, where she explains that "data privacy law can this be defined as a set of measures aimed at safeguarding data subjects from harm resulting from the computerised or manual processing of their personal information by data controllers."

[63] *Investigating Directorate: Serious Economic Offences and others 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).

space and proceeded to criticise the decision taken by the court in *Bernstein v Bester*[64] on the basis that, there is movement away from a person's intimate core as privacy is no longer retained in the interaction of social capabilities.[65] This case demonstrates the willingness of the Constitutional Court to protect the right to data privacy, specifically in the light of technological advances, which increase the capability to collect, intercept or disseminate personal information without an individual's consent and therefore without their control, thereby directly impacting on the protection of such right.

In the face of rapid technological advancements, at the heart of this discussion is the assertion that protection of data privacy by SA law should be adequate to safeguard data subjects from the risks emanating from the unlawful processing of their personal data and further to ensure that they have active control over the use of, collection or disclosure of their personal information. This Chapter therefore examines the effectiveness of the current data protection legal regime in SA. In so doing, the country's common law, the Constitution and the POPIA are critically analysed to contextualise the level of protection afforded to data privacy in SA.

2.2 SOUTH AFRICAN COMMON LAW

2.2.1 Privacy Protection

In general, privacy is protected as an independent right of personality under the law of delict.[66] Watermeyer J, in *O'Keeffe v Argus Printing and Publishing Co Ltd*,[67] broadened the meaning of the concept of *dignitas* to encompass all aspects of the personality rights which are protected, with the exception of bodily integrity (*corpus*) and reputation (*fama*).[68] Therefore, the collective nature of the concept of *dignitas* integrates the right to privacy with all other personality rights and the right to privacy is not a stand-alone right. For protection

[64] Supra note 58.

[65] Ibid at 16. The Constitutional Court expanded on the definitional nature of the right to data privacy by asserting that "when people are in their offices, in their cars or on mobile telephones, they still retain a right to be left alone by the state unless certain conditions are satisfied …Wherever a person has the ability to decide what he or she wishes to disclose to the public and the expectation that such a decision will be respected is reasonable, the right to privacy will come into play."

[66] A Roos 'Personal data protection in New Zealand: lessons for South Africa?' (2008) 4 *Potchefstroom Electronic Law Journal* 90.

[67] 1954 (3) SA 244(C).

[68] Y Burns and A Burger-Smidt *A Commentary on the Protection of Personal Information Act* (2018) 2.

to be afforded, the test is subjective, in that a person must determine whether his or her private information should not be disclosed to others.[69]

Hence, at common law, a third party will be liable for invading the privacy of another if the violation of information is secret, private or confidential in nature. Neethling is of the opinion that the right to privacy embodied as a personality right is not absolute, but is limited by the lawful interests of others and interests of the public.[70] The common law, therefore, does not recognise privacy as a separate right and the test for infringement thereof is too subjective to afford a person a high degree of protection from privacy intrusions. For instance, since personal data is regarded as a valuable commodity, it can be argued that the right to data privacy itself may be limited by the financial interests of the company exploiting the personal information for commercial gain or it may be in the public interest, leaving the aggrieved party without effective legal redress.

2.2.2 Remedies for Privacy Infringements

Unlawful processing of personal data by technological means infringes data privacy when the personal data is used, collected, stored or disclosed without a person's knowledge or consent or when security measures fail to prevent the disclosure thereof.[71] It has been argued that the South African common law has taken a casuistic approach to privacy covering categories of privacy infringements, such as unreasonable or unlawful intrusion of a person's private space or publically disclosing private facts about a person.[72]

Therefore, privacy infringements amount to an *iniuria*, for which remedies are available to a person seeking relief under the law of delict as follows: -

(a) *actio iniuriarum*

Under the requirements of the *actio iniuriarum*, a claim for non-patrimonial loss may be instituted. The plaintiff must show that a personality right was intentionally violated in a

---

[69] J Neethling et al *Neethling's Law of Personality* (note 59 above) 240.
[70] J Neethling et al *Neethling's Law of Personality* (note 59 above) 281.
[71] SALRC Final Report (note 19 above) 19.
72 JM Burchell *Principles of Delict* 1ed (1993) 208. See further, *Financial Mail (Pty) Ltd v Sage Holdings Ltd* (1993) ZASCA 3; 1993 2 SA 451 (A) 462F, where the court identified two instances of privacy invasion, namely, "an unlawful intrusion upon the personal privacy of another or the unlawful publication of private facts about a person."

wrongful manner.[73] Hence, the defendant's negligence alone does not attract liability in terms of the law of delict. Wrongfulness is determined by weighing up the conduct with the *boni mores*; if the *boni mores* regards such as unreasonable, the conduct will be regarded as wrongful.[74] The defendant will need to rebut two presumptions, namely, that the conduct is wrongful and conducted intentionally.[75] These presumptions can further be rebutted if the defendant can prove it was done mistakenly.[76] Since certain technologies are used to process personal data without a plaintiff's consent or knowledge, this remedy can only be invoked if the plaintiff is aware of the wrongful and intentional conduct of unlawful processing of his or her personal information.

(b) *actio legis aquiliae*

The plaintiff can claim patrimonial loss for the processing of personal information which occurred wrongfully, intentionally or negligently, thereby infringing the plaintiff's right to privacy. Unlike the *actio iniuriarum,* under the aquilian action, negligence is sufficient to establish liability for damages.[77]

(c) Interdict

An interdict is available to avert the wrongful processing of personal information or to prevent the continuation thereof.[78]

From the foregoing, the common law and its remedies do not afford a person an element of control over their personal data.[79] Neethling convincingly argues that the common law is not effective to address the infringement of privacy rights caused by unlawful

[73] A Roos 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position' (note 2 above) 197.
[74] Ibid.
[75] A Roos 'Data Protection Law in South Africa' (note 56 above), explains with reference to Neethling's *Law of Personality* that "the presumption of wrongfulness can be rebutted by proving that a ground of justification, such as private defence, necessity, provocation, consent to injury and exercise of a statutory right or official authority was present…the presumption of intent can be rebutted by proving that the publication was done mistakenly."
[76] J Neethling et al *Neethling's Law of Personality* (note 59 above) 63.
[77] Ibid at 254.
[78] Ibid.
[79] Ibid at 278.

processing of personal data and that statutory data protection is required.[80] Neethling calls for "active control principles" [81] which are deficient in the common law protection of personality rights. Roos shares the same view.[82]

In my view, the common law is deficient to specifically protect data privacy infringements in that case law applying the common law principles demonstrates that liability for infringing the right to privacy is confined to information (not necessarily personal information) which a person perceives to be private. The common law does not allow an individual to actively take control of his or her personal information. In light of the challenges posed by technological advancements, a further downside to the delictual principles is that a person cannot hold another liable where his or her personal information is processed negligently.

2.3 CONSTITUTIONAL PROTECTION

Constitutional protection of a person's privacy emanates from the fundamental right not to have the privacy of their communications infringed,[83] which is of particular importance to data protection.[84] Currie and De Waal focussed on the *Mistry v Interim Medical and Dental Council of South Africa* case and noted that the Constitutional Court expanded on the privacy rights contained in the Constitution to protect "informational self-determination".[85] Cases involving the violation of data privacy have not been extensively dealt with by the Constitutional Court. The Constitutional Court in *Mistry v Interim Medical and Dental Council of South Africa*[86] attempted to formulate guidelines to determine if there has been an infringement of data privacy.

However, the Constitution merely creates a broad framework for data privacy. A full framework of data protection principles cannot be left to the Constitutional Court to develop

---

[80] J Neethling et al *Neethling's Law of Personality* (note 59 above) 281.
[81] J Neethling et al *Neethling's Law of Personality* (note 59 above) 278.
[82] A Roos 'Data Protection Law in South Africa' (note 56 above) 200.
[83] Section 14(d) of the Constitution.
[84] In *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC), it was held that although not expressly stated in the then section 13 of the Interim Constitution, the right to informational privacy is covered by the broad protection of privacy guaranteed by section 13.
[85] I Currie et al *The Bill of Rights Handbook* 6ed (2013) 302-303. The authors explain that informational self-determination is "an interest in restricting the collection, use of and disclosure of personal information."
[86] See Mistry v *Interim Medical and Dental Council of South Africa* (note 84 above) at 51.

because it is the task of the legislature to give effect to a legislated data protection regime in SA.

2.4 STATUTORY DATA PROTECTION

2.4.1 Sectoral-specific legislation

Sectoral laws enacted in the form of the PAIA,[87] the Electronic Communications and Transactions Act No. 25 of 2002 (ECTA)[88] and the National Credit Act (NCA)[89] provide limited protection of data privacy in SA.[90] Although the PAIA[91] gives effect to data privacy by enabling persons to access and correct their personal information contained in manual and electronic records, it promotes freedom of information and is not a comprehensive data protection statute.[92]

The main objective of the ECTA is to protect the public interest by facilitating electronic communications and transactions.[93] This Act does not impose mandatory obligations on data controllers, compliance with section 51 is voluntary, no independent supervisory body exists and there are no criminal penalties to enforce compliance with the principles.[94] The POPIA trumps the ECTA by providing for mandatory data protection principles.

In respect of the NCA, "confidential information",[95] is defined to include personal information. However, data protection in the NCA is confined to the consumer credit industry.[96] As with the ECTA, the lacuna in the NCA is that it does not contain specific data protection obligations to safeguard data privacy in particular.

---

[87] No. 2 of 2000.
[88] No. 25 of 2002.
[89] No. 34 of 2005.
[90] A Roos 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position' (note 2 above) 424.
[91] One of the objectives of the PAIA set out in section 9(b)(1) is to "give effect to the constitutional right of access to any information held by the state or by another person - subject to justifiable limitations, including, but not limited to, limitations aimed at the reasonable protection of privacy."
[92] Ibid.
[93] Section 2(1) of the ECTA.
[94] A Roos 'Data Protection Law in South Africa' (note 56 above) 428-429.
[95] Section 1 of the NCA.
[96] Section 3 of the NCA.

The protection afforded by the sectoral legislation referred to above offers rather fragmented protection of data privacy. The broader yet more specific protection of personal information was therefore assessed against sectoral legislation to guard against over-regulation but also to ensure that the generic protection of a data protection regulatory regime is implemented in tandem with sector specific legislation.[97]

2.4.2 Specific Data Protection: The POPIA

2.4.2.1 Overview of the POPIA

A brief background of the enactment of the POPIA is presented in Chapter 1 above.[98] The focus of the discussion here is the specific provisions of this Act that aim to safeguard the constitutionally protected right to data privacy.[99] It is apt to note that greater legislative protection is required to counteract vulnerabilities to privacy caused by the disruption of the economic climate facilitated by global trade and technological developments.[100] The effects of the current technological era on personal data were noted by Willis J in *H v W*,[101] who contended that the common law needs to be developed where infringements of privacy take place in social networking.[102]

The journey to the POPIA commenced with the SALRC embarking on a lengthy and time-consuming process to investigate legislative reform.[103] With a focus on the technological risks that impact personal data protection, the SALRC highlighted that the ease of electronic communication through the modes of ICT and the internet, increased privacy infringements and required countries to either establish or revise data protection legislation.[104]

---

[97] SALRC's Discussion Paper 109 (Project 124) (note 15 above) 396.
[98] See Chapter 1, paragraph 1.1 above.
[99] The SALRC Final Report (note 19 above) at 3.3.43 explains that "the aim of privacy legislation is not to stem the flow of information, but to regulate it."
[100] Y Burns and A Burger-Smidt *A Commentary on the Protection of Personal Information Act* (note 68 above) 4-5.
[101] (2013) 2 All SA 218 (GSJ).
[102] Ibid at 21.
[103] The SALRC Final Report (note 19 above) at 1.3.1.
[104] SALRC Final Report (note 19 above) at 4.1.1-4.1.3.

The SALRC's investigation included an extensive analysis of data protection law in well-established foreign jurisdictions.[105] However, it is widely accepted that the POPIA is premised on the EU legal regime for data protection.[106] It was assumed that the POPIA would become operational once the office of the Information Regulator was established and the POPIA Regulations were issued.[107] Despite the Information Regulator having being established and the gazetting of the draft POPIA Regulations,[108] at the time of submission of this study, the POPIA Act had still not entered into full force and effect,[109] with some authors of the view that such delay was due to the publication of the draft EU General Data Protection Regulation (GDPR).[110]

2.2.4.2 Objectives and Application of the POPIA

Section 2 of the POPIA encapsulates its primary objectives. The limitation contemplated in this section will require that a balance be struck between the right to privacy and the right of access to information and the interests of free flow of information within and outside SA's borders.[111] Luck posits that the right to privacy, although fundamental, may be limited and balanced, taking into account that data privacy is not confined to domestic policy but is part of the global community and therefore economic and trade considerations come into play.[112]

As discussed in sub-section 2.2.4.1 above, the POPIA was developed around the European data protection regulatory regime; therefore, another important objective is to ensure that its conditions for lawful processing are in harmony with international

---

[105] The comparative legal jurisdictions investigated included the United Kingdom, Ireland, Canada, Australia, the United States of America, the Netherlands, New Zealand and Chile.

[106] The SALRC Final Report (note 19 above) dealt extensively with the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and Directive No. 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 Free Movement.

[107] A Roos 'Data Protection Law in South Africa' (note 56 above) 202-203.

[108] See the discussion on the Information Regulator and the POPIA Regulations in Chapter 1, paragraph 1.1 above.

[109] See discussion in Chapter 1, paragraph 1.1 for an update on the status of the promulgation of the remaining provisions of the POPIA.

[110] D Milo and G Palmer 'South Africa- New comprehensive data privacy law passed' *Linklaters* 31 January 2014, available at *http://www.linklaters.com/Insights/Publication1403Newsletter/TMT-News-31-January-2014/Pages/SouthAfrica-New-comprehensive-data-privacy-lawpassed.aspx*, accessed on 20 June 2019.

[111] Section 2 (a) (i) and (ii) of the POPIA.

[112] R Luck 'POPI - is South Africa keeping up with international trends?' (2014) 44 *De Rebus* 84.

standards.[113] Furtherance of this objective is linked to the Information Regulator's mandate in terms of section 40(e) of the POPIA.[114]

The POPIA applies to the processing of personal information where the information is entered in a record[115] by or for a responsible party[116] by making use of automated or non-automated means.[117] The Act also applies where the responsible party resides in SA, suggesting it does not have extraterritorial scope of application.[118] The POPIA applies to a responsible party not domiciled in SA, but who utilises automated or non-automated means in SA, unless those means are used to only forward personal information through SA.[119]

2.2.4.3 Key Terms used in the POPIA

The key terms used in the POPIA include "personal information", "processing"[120], "data subject"[121] and "responsible party"[122]. Without going into detail, for the purposes of this study, the terms "personal information" and "processing" are important for determining the protection afforded to data privacy. "Personal information" is broadly defined[123] and as such biometric data, internet protocol addresses and cookie identifiers fall within its definition.[124]

The term "processing" is also given a broad meaning to cover any action performed by a third person on personal information. Protection of data privacy is therefore dependant

---

[113] Section 2(b) of the POPIA.

[114] This function of the Information Regulator is discussed further in Chapter 3.

[115] Section 1 of the POPIA defines a 'record' in broad terms.

[116] Section 1 of the POPIA defines a 'responsible party' as "a 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."

[117] Section 3(1) of the POPIA. The term 'non-automated means' is not defined in the POPIA.

[118] Unlike the territorial scope of the POPIA, the GDPR applies to organisations based outside the EU, that target EU citizens. See discussion in Chapter 5, paragraph 5.2.2.2 below.

[119] Section 3(1) (b) (ii) of the POPIA. See Y Burns and A Burger-Smidt *A Commentary on the Protection of Personal Information Act* (note 68 above) at 6. The authors are of the view that in this regard, "the responsible party will not be considered to have processed the personal information: he, she or it is acting as a mere conduit for the forwarding of personal information, this occurs where the responsible party forwards personal information from one country to another and the information is routed by way of automated or non-automated means through the Republic."

[120] See note 21 above for the definition of 'processing'.

[121] See note 43 above for the definition of a 'data subject'.

[122] Section 1 of the POPIA defines a 'responsible party' as "a 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."

[123] Section 1 of the POPIA.

[124] A Roos 'Data Protection Law in South Africa' (note 56 above) 204.

on the responsible party lawfully processing the data subject's personal information in compliance with the eight conditions[125] discussed below.

2.2.4.4 Conditions for the Lawful Processing of Personal Information

The POPIA contains the following eight conditions[126] for lawful processing by the responsible party:

(a) Condition 1: Accountability

The responsible party must ensure that all the conditions set out in Chapter 3 of the Act are complied with at the point when the purpose, collecting the personal information and during the processing itself is determined. Accountability is a thread running through the POPIA and the responsible party must remain accountable at every stage of the processing.[127]

(b) Condition 2: Processing Limitation

Condition 2 sets limits regarding the reasons for processing, which include the lawfulness of processing, minimality, consent, justification and objection and collection directly from the data subject.

(i) Lawfulness of processing[128]

Processing must be done lawfully and reasonably without infringing privacy rights. This requirement is not confined to the POPIA but extends to ensuring compliance with other laws such as the Constitution, other legislation and international instruments to which SA is a signatory.[129]

[125] Y Burns and A Burger-Smidt *A Commentary on the Protection of Personal Information Act* (note 68 above) 29.
[126] Chapter 3 of the POPIA.
[127] Y Burns and A Burger-Smidt *A Commentary on the Protection of Personal Information Act* (note 68 above) 45.
[128] Section 9 of the POPIA.
[129] Y Burns and A Burger-Smidt *A Commentary on the Protection of Personal Information Act* (note 68 above) 48.

(ii) Minimality[130]

To qualify for processing, personal information must be adequate, relevant and not excessive, given the purpose of its intended use. It has been argued that the literal interpretation of section 10 requires that all three requirements (adequate, relevant and not excessive) should be met for the processing to be regarded as lawful.[131] For the avoidance of doubt and interpretational issues, the minimality requirement should be confined to the specific purpose which must be necessary to collect the personal information.

(iii) Consent, justification and objection

The POPIA defines "consent" as "any voluntary specific and informed expression of will in terms of which permission is given for the processing of personal information".[132] It has been argued that technology creates a barrier to free and informed consent. For example, Big Data enables data to be reused outside the purpose limitation for which consent was obtained and as such threatens the function and significance of consent as a legal ground.[133] A holistic approach must be adopted to privacy standards in order to enhance the consent requirement by embedding privacy by default or privacy by design standards,[134] which is not a requirement in the POPIA.

(iv) Collection directly from the data subject[135]

The final requirement of the processing limitation is that the personal information must be collected directly from the data subject in order to ensure that the data subject is in control of the processing. The POPIA thus provides better protection than common law to ensure active control. However, there are exceptions to this provision which dilute its effect.[136]

[130] Section 10 of the POPIA.
[131] Y Burns and A Burger-Smidt *A Commentary on the Protection of Personal Information Act* (note 68 above) 51.
[132] Section 1 of the POPIA.
[133] L Mitrou 'The General Data Protection Regulation: A Law for the Digital Age?' in Tatiana-Eleni Synodinou et al (ed) *EU Internet Law*: Springer (2017) 39-40.
[134] Ibid at 42.
[135] Section 12(1) of the POPIA.
[136] The exceptions are set out in section 12(1)(2) of the POPIA.

(c) Condition 3: Purpose specification

Collection of the personal information must be explicitly defined and relate to a lawful purpose linked to an activity or function of a responsible party.[137] This requirement covers the full lifecycle of processing the personal information in relation to the specific purpose for which it is collected. The responsible party will be required to inform that data subject of the purpose from the time of collection of the personal information right through to the destruction thereof.

However, given the requirements of section 14(3) of the POPIA, personal information could be retained for several years.[138] The responsible party is required to destroy, delete or de-identify a record it as soon as is reasonably practicable once the retention thereof is no longer authorised in terms of section 14 (1) and (2).[139]

(d) Condition 4: Further processing limitation

Further processing of personal information must be in accordance or compatible with the original purpose for which it was collected in terms of section 13.[140] Compatibility is determined by taking into account certain factors listed in section 15(2) of the POPIA.[141] Further processing is not regarded as incompatible with the initial intended purpose of collection if any one of the factors contained in section 15(3)(a) to (f) are met.

(e) Condition 5: Information Quality

In terms of section 16 of the POPIA, a responsible party is required to ensure that the personal information is complete, accurate, not misleading and updated, by taking reasonably

[137] Section 13(1) of the POPIA.

[138] The POPIA allows the responsible party, in the absence of a law or a code of conduct, to retain the record for a period which will afford the data subject a reasonable opportunity to request access to the record. Subject to the establishment of appropriate safeguards against the records being used for any other purposes, records of personal information may be retained for longer periods for historical, statistical or research purposes.

[139] Section 14(4) of the POPIA.

[140] Section 15(1) of the POPIA.

[141] Section 15(2) of the POPIA.

practicable steps.[142] In this regard, the purpose for which personal information is collected or further processed must be taken into account by the responsible party.[143]

(f) Condition 6: Openness

A responsible party has an obligation to maintain documentation relating to all processing operations under its responsibility as referred to in sections 14 or 51 of the PAIA.[144] Section 18(1), which is similar to section 13(1), requires the responsible party to take reasonably practicable steps to make the data subject aware of the details of the personal information collected.[145]

(g) Condition 7: Security Safeguards

In terms of this condition, in order to secure the integrity and confidentiality of personal information, the responsible party must take appropriate, reasonable technical and organisational measures to prevent loss, damage or destruction thereof and against unlawful access to or processing of personal information.[146] Technical and organisational measures require risk identification prior to safeguards being implemented.[147] The draft POPIA Regulations therefore demonstrate that the Information Regulator is leaning towards a risk-based approach to POPIA compliance. [148]

This condition contemplates self-regulation and may not be sufficient to counter the effects of modern digital technologies which have the potential to bypass security mechanisms put in place by the responsible party. It is a novelty and is also not recognised in terms of traditional common law principles. However, the POPIA does not include the obligation (design and default) to ensure that privacy safeguards are 'built in' to the

[142] Section 16(1) of the POPIA.
[143] Section 16(2) of the POPIA.
[144] Section 17 of the POPIA.
[145] The list of the details is enumerated in section 18(1) (a) to (h) of the POPIA. See further J Neethling 'Features of the Protection of Personal Information Bill' (2013) 75 Journal of Contemporary Roman-Dutch Law 241-255.
14, where he points out that this condition forms the basis for effective control by data subjects of the processing of their personal information and further indicates that the principle of openness is not known at common law.
[146] Section 19(1)(a) and (b) of the POPIA.
[147] Section 19(2) of the POPIA.
[148] Regulation 4 of the draft POPIA Regulations.

technology from the design stage; ideally, such provision should be made under the accountability condition of the POPIA.[149]

(h) Condition 8: Data subject participation

This condition flows from the openness principle and grants the data subject two specific rights to actively control their personal information, namely, the right of access to their personal information and the right to correct or delete it. The common law does not provide the data subject with such right.

2.5 CONCLUDING REMARKS

It has been argued that the principles of the law of delict provide limited protection of data privacy since active control by the data subject of the processing of personal data is not recognised. Specific protection of data privacy has not been recognised by the courts applying traditional delictual principles in cases involving privacy infringement.[150] The examination of the constitutional provision relating to the right to privacy demonstrates that data privacy is not explicitly provided for in section 14; however, case law shows that the Constitutional Court has extended protection of privacy to informational (data) privacy. Neethling's sentiment must be echoed in that the legislature is obliged in terms of the Constitution to pass data protection legislation.[151]

The active control principles contained in the POPIA are unique to a data protection regulatory regime. It was demonstrated that the POPIA goes beyond common law protection of privacy by safeguarding the data subject's rights which are inherent in the conditions for lawful processing.[152] The authors of a recent article that examines the case *Black Sash Trust v Minister of Social Development*[153] explain the misuse and unlawful processing of social security personal information and call for the POPIA to come into full force and effect to enable the Information Regulator to become fully operational and exercise its enforcement

[149] Condition 1, which is discussed in paragraph 2.2.4.4 (a) above.

[150] A Roos 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position' (note 2 above) 422.

[151] J Neethling et al *Neethling's Law of Personality* (note 59 above) 17.

[152] J Neethling 'Features of the Protection of Personal Information Bill' (note 145 above) 14.

[153] *Black Sash Trust v Minister of Social Development and Others (Freedom Under Law NPC Intervening*) (CCT48/17) [2017] ZACC 8; 2017 (5) BCLR 543 (CC); 2017 (3) SA 335 (CC).

powers to protect against privacy infringement.[154] The following Chapter explores the adequacy and effectiveness of the POPIA enforcement and penalty regime.

[154] B Batchelor and T Wazvaremhaka 'Balancing financial inclusion and data protection in South Africa: *Black Sash Trust v Minister of Social Development'* (2019) 136(1) *SALJ* 112.

CHAPTER 3: AN EVALUATION OF THE POPIA ENFORCEMENT MECHANISMS AND PENALTY REGIME TO ADDRESS TECHNOLOGICAL ADVANCEMENTS

3.1 INTRODUCTION

The SALRC's analysis of a data protection regime identified three elements that are required for adequate enforcement of a data protection system.[155] This Chapter explores the POPIA's enforcement and penalty regime and critically evaluates whether this Act contains adequate and effective enforcement actions to address interference with data protection. It also examines whether the POPIA's penalty regime is appropriate to enforce data privacy breaches. In this regard, the oversight and enforcement role of the Information Regulator is explored.

3.2 OVERSIGHT AND ENFORCEMENT STRUCTURE

The POPIA is premised on the core elements for the external supervision of data protection legislation recommended by the SALRC.[156] It features a regulatory or co-regulatory system[157] rather than a self-regulatory system[158] to enforce the data protection principles.[159] For instance, as demonstrated in *Ketler Investment CC Presentations v Internet Service*

---

[155] These elements include an adequate level of compliance with the data protection conditions; a system which provides support and assistance to data subjects to exercise their rights; and the provision of adequate remedies to the aggrieved party where such rules have been violated. See SALRC Final Report (note 19 above) 406.

[156] Refer to SALRC Final Report (note 19 above) at 6.8.1 where the following core elements were recommended:

> "(a) an independent oversight body is tasked with powers to investigate and to participate in legal actions where data protection legislation is violated;
>
> (b) data subjects are able to enforce compliance to data protection legislation independently to an information regulator by approaching a court or appealing any decision taken by the person processing the personal data or the information regulator;
>
> (c) an aggrieved party suffering damages due to breach of data protection legislation is entitled to recourse by initiating a claim for compensation from the offending party; and
>
> (d) there are several criminal offences for non-compliance thereto."

[157] The regulatory or co-regulatory system makes provision for external supervision by an independent authority having oversight in respect of enforcement. Refer to the SALRC Final Report (note 19 above) at 8.1.5.

[158] Ibid. The SALRC explained that in a self-regulatory system, there is no independent authority, such as the Information Regulator, to oversee compliance to data protection and consequently the parties processing personal data will have the discretion to determine how to comply with such legislation. The data subject will then need to approach the courts to enforce his or her rights under such legislation dealing with data protection. The ECTA is an example of a self-regulatory system.

[159] SALRC Final Report (note 19 above) at 6.1.2, where it is specifically indicated that the focus was on the enforcement actions of data privacy in the narrow sense which could either be initiated based on a breach of data protection legislation through complaints or by oversight authorities through their own investigation and audit programme. See further G Greenleaf. (2013a). Chapter 10: 'Data protection in a globalised network' in Brown, 1 (ed) *Research handbook on governance of the Internet.* Northampton, MA: Edward Elgar 221- 259, where the author recommends that an effective data protection regime should include the establishment of an independent

Providers' Association, the self-regulatory system contained in the ECTA failed.[160] The POPIA seeks to address the deficiencies in the ECTA by protecting data subjects where, for instance, spam is sent without the data subject's consent.[161]

Ensuring that technical expertise is part of the Information Regulator's structure is also critical since data protection as a whole and ICT expertise, in particular, have been described as "moving targets" due to existing technologies and the rapid rate at which emerging technologies are likely to flourish.[162]

3.3 ENFORCEMENT MECHANISMS

The enforcement procedures set out in Chapter 10 of the POPIA are triggered by any interference with the data protection rights afforded to a data subject. In terms of section 73 of the POPIA, such interference is triggered in the following instances:

(a) any breach of Chapter 3 comprising of the conditions for lawful processing of personal information;
(b) failure to comply with sections 22,[163] 54,[164] 69,[165] 70,[166] 71[167] or 72;[168] or
(c) a breach of any aspect of a code of conduct issued in accordance with section 60.

The application of the above-mentioned sections is wide enough to cover infringement of data protection rights caused by technologies used to process such personal information,

---

DPA to enforce data protection law, carry out investigations of privacy complaints and to ensure that data privacy legislation is improved and amended.

[160] *Ketler Investment CC Presentations v Internet Service Providers' Association* 2014 (1) ALL SA 566 (GSJ) ("Ketler case").

[161] In the Ketler case, the court determined that section 45 of the ECTA allowed spamming through self-regulation, which resulted in the defamation of the applicant. Unlike the ECTA, the POPIA will specifically hold a wrongdoer liable to ensure that the consent of a data subject is obtained prior to sending unsolicited communication or direct marketing and the Information Regulator is vested with the power to ensure it conducts research to stay abreast of the moving target nature of technology. The court in the Ketler case accordingly acknowledged that the Protection of Personal Information Bill seeks to address spam "in a manner that requires some form of relationship to exist between the sender and recipient or some other adequate connection and is therefore more restrictive on spam activities than section 45 of ECTA."

[162] C Raab and I Szekely 'Data Protection Authorities and Information Technology' *Computer law & Security Review* (2017) 33 421–33.

[163] Section 22 of the POPIA deals with notification of security compromises.

[164] Section 54 of the POPIA deals with the duty of confidentiality.

[165] Section 69 of the POPIA deals with direct marketing by means of unsolicited electronic communications.

[166] Section 70 of the POPIA deals with printed or electronic directories.

[167] Section 71 of the POPIA deals with automated decision making.

[168] Section 72 of the POPIA deals with transfers of personal information outside the Republic.

particularly the POPIA conditions relating to consent and technical safeguards, which new technologies fall short of meeting. Where a code of conduct is developed to regulate the use of certain technologies, any breach thereof will result in interference with data protection rights.[169]

3.3.1 Complaints

Section 74 of the POPIA provides that any person is entitled to lodge a complaint with the Information Regulator with regard to any alleged interference with data protection rights.[170] The complaint has to be lodged in a prescribed manner and form.[171] It must be lodged in writing[172] and the Information Regulator is required to provide assistance as may be reasonably necessary to enable the complainant to do so.[173] Burns and Burger-Smidt[174] submit that the wide *locus standi* in terms of section 74 allows a third party to act for and on behalf of the data subject or responsible party, which is consistent with the Constitution.[175]

On receipt of a complaint, the Information Regulator can proceed with any of the actions set out in section 76(1)(a) to (f).[176] On completion of an investigation, the Information Regulator may decide not to proceed with any action only if it is of the opinion that one of the grounds referred to under section 77(1)(a) to (f) applies. The Information Regulator is also given discretionary powers not to take any further action.[177] However, in either case, the Information Regulator is required to inform the complainant of its decision and the reasons.[178] The complainant may challenge the rationality and reasonableness of the

[169] Sections 60 to 68 of the POPIA set out the requirements for developing codes of conduct.
[170] Section 74(1) of the POPIA.
[171] Regulation 7 (1) of the POPIA Regulations provides that Part I of Form 5 must be used to submit a complaint to the Regulator.
[172] Section 75(1) of the POPIA.
[173] Section 75(2) of the POPIA.
[174] Y Burns and A Burger-Smidt *A Commentary on the Protection of Personal Information Act* (note 68 above) 220.
[175] Section 38 of the Constitution deals with enforcement of rights and representation by persons who may approach the court for relief if any right contained in the Bill of Rights has been violated.
[176] These actions include conducting pre-investigations, acting as conciliator in a matter involving infringement of data protection rights, fully investigating a complaint, taking no action (after considering the factors in section 77 of the POPIA) or referring the compliant to the Enforcement Committee.
[177] Section 77(2) of the POPIA.
[178] Section 77(3) of the POPIA.

Information Regulator's decision[179] by taking the matter on judicial review to a court in terms of the Promotion of Administrative Justice Act.[180]

In conducting investigations in relation to complaints, the Information Regulator has broad powers that are equivalent to those of the High Court.[181] By virtue of such powers, aggrieved parties may be more reluctant to approach the Court directly for relief; this would thus enhance the Information Regulator's function of enforcing data protection.

3.3.2 Warrants for search and seizure

In terms of section 82 of the POPIA, the Information Regulator may apply to the High Court or Magistrates Court for a warrant to enter and search premises in its area of jurisdiction only upon satisfaction of the reasonable grounds referred to in section 82 (1) of the Act.[182] The Information Regulator has seven days from the date of the warrant to conduct the search, inspection, examination, operation and testing of any record, material equipment or device which is being used or will be used to process personal information and further to seize the offending record, material, equipment or device to be used as evidence.[183] However, the use of certain technologies such as the Cloud to store personal data outside SA will create jurisdictional challenges for the Information Regulator in exercising its search and seizure powers.

Thus, while the POPIA's provisions aim to circumvent violation of the constitutionally protected right to privacy by providing detailed requirements for the issuing as well as lawful execution of a warrant,[184] where personal information is transmitted and stored outside of SA (such as Cloud services), the search and seizure relief will not be appropriate due to the lack of jurisdiction.

---

[179] Y Burns and A Burger-Smidt *A Commentary on the Protection of Personal Information Act* (note 68 above) 223.

[180] No. 3 of 2000. See section 6.

[181] Section 80 of the POPIA.

[182] These grounds include interference with data protection rights or instances where an offence under the POPIA is being committed or will likely be committed.

[183] Section 84 of the POPIA.

[184] Sections 83 and 84 of the POPIA.

3.3.3 Assessment

A further enforcement mechanism is the assessment (audit) procedure the Information Regulator may conduct to determine if the processing complies with the POPIA.[185] The procedural requirements for conducting assessments are dealt with in terms of Regulation 11 of the POPIA Regulations.[186] Upon completion of an assessment, the Information Regulator must issue a report on the results and any recommendations arising therefrom.[187] This report has the force of an enforcement notice (discussed in paragraph 3.3.4 below).[188]

3.3.4 Enforcement Committee and Enforcement Notices

The POPIA allows the Information Regulator to refer a complaint or any other matter (after investigation by the Information Regulator) to the Enforcement Committee,[189] to consider a finding with regard to a complaint, any other matter or a recommendation concerning the intended action to be taken by the Regulator.[190] Upon completion of the Enforcement Committee's investigation, the Information Regulator could elect to serve an enforcement notice on the responsible party for interfering with the complainant's personal information.[191] The POPIA allows the responsible party to appeal against an enforcement notice within 30 days of receipt of such notice.[192]

The POPIA[193] requires that the Information Regulator appoint an Enforcement Committee comprised of a person with specialist knowledge of matters relating to the work of the Information Regulator to assist and advise the Regulator to perform its functions under

---

[185] Section 89 of the POPIA.

[186] In terms of Regulation 11, Part 1 of Form 11 must be used to "request an assessment from the Information Regulator, Part II of Form 11 is used by the Information Regulator to inform the requester of its decision to conduct the assessment on its own accord or by any person requesting the assessment and Form 12 must be completed by the Information Regulator to notify the requester or the responsible party of any decision, action or view taken".

[187] Section 91(1)(a) and (b) of the POPIA.

[188] Sections 91(3) and 95 of the POPIA.

189 The Terms of Reference of the Enforcement Committee were signed on 18 April 2019 at 1.2. available at *https://www.justice.gov.za/inforeg/docs/InfoRegSA-TOR-EFcommittee.pdf,* accessed on 12 August 2019.

[190] Section 92(1) of the POPIA.

[191] Section 95(1) of the POPIA. The enforcement notice serves as a directive for the responsible party to either implement steps or to refrain from implementing steps or prohibit the unlawful processing in accordance with the manner and time period specified in the enforcement notice. See further section 95(1)(a) and (b) of the POPIA.

[192] Section 97 of the POPIA.

[193] Section 50(1)(b) of the POPIA.

the POPIA.[194] However, it is not clear from the Terms of Reference of the Enforcement Committee[195] whether a person with ICT expertise should be appointed. In any event, section 47(7) of the POPIA only requires the Information Regulator to appoint a person with specialist knowledge on a temporary basis.

3.3.5 Civil Remedies

Civil proceedings may be instituted by the data subject against a responsible party for contravening the provisions of the POPIA.[196] The Act creates statutory liability, meaning that intention or negligence need not be proved by the data subject in a claim for damages against the responsible party. The responsible party may rely on the defences specified in Section 99(2)(a) to (e) of the POPIA.[197]

The Information Regulator may also institute civil action on behalf of the data subject, if requested to do so.[198] Any contravention of the POPIA by the responsible party, will entitle the data subject to claim damages suffered as compensation for patrimonial and non-patrimonial damages.[199] Aggravated damages, interest and the costs of the suit may also be claimed by the data subject.[200]

By creating statutory liability for responsible parties, the POPIA provides an adequate and effective enforcement mechanism through civil remedies.

3.4 PENALTY REGIME

3.4.1 Offences and Penalties

The POPIA provides for offences for contravention, for which fines or imprisonment can be imposed on the wrongdoer. The penalties imposed can be categorised into "serious

[194] Section 47(7) of the POPIA.
[195] See note 189 above.
[196] Section 99 of the POPIA.
[197] The defences available to the responsible party include, vis major; consent and fault on the part of the plaintiff; compliance could not be reasonably achieved in the circumstances; or an exemption in terms of section 37 was granted by the Information Regulator.
[198] Section 99(1) of the POPIA.
[199] Section 99(3) (a) of the POPIA.
[200] Section 99(3) (b), (c) and (d) of the POPIA.

offences"[201]and "less serious offences".[202] Conviction for serious offences renders the offender liable to a fine or imprisonment of up to 10 years, or both.[203] On conviction for a less serious offence, a person is liable to a fine or imprisonment for a period of up to 12 months, or both.[204] A Magistrates Court has jurisdiction to impose these penalties in terms of section 108 of the POPIA.

3.4.2 Administrative Penalties

In place of criminal proceedings, the POPIA provides an option for a person committing an alleged offence to pay an administrative fine. This is subject to the discretion of the Information Regulator upon service of an infringement notice on the offending party.[205] The administrative fine must be payable within the time period stipulated in the infringement notice and it becomes recoverable if the offender fails to comply with any stipulation in such notice.[206] The Information Regulator can then file a statement with the clerk or registrar of any competent court setting out the quantum of the administrative fine payable by the offending party.[207] The statement will have the effect of a civil judgment in favour of the Information Regulator for a liquid debt of the amount stipulated in the statement.[208]

Serious offences for which a higher penalty can be imposed should include the processing of personal information caused by the ill-effects of technologies; for instance, where personal information is processed without consent or where it is intentionally or negligently re-identified after it has been de-identified.

---

[201] Serious offences committed by the responsible party include hindering, obstruction or unlawfully influencing the Information Regulator, or a person acting on its behalf, in the performance of the Information Regulator's duties and functions under the POPIA; failure to comply with an enforcement notice served in terms of section 95; knowingly giving false evidence to the Information Regulator on the basis of a sworn statement or affirmation; unlawful processing of an account number of a data subject; knowingly or recklessly, without the data subject's consent, obtaining or disclosing an account number of a data subject to another person; selling an account number, or offering to sell the account number of a data subject.

[202] Less serious offences include failure to notify the Information Regulator of processing without prior authorisation; a breach of the duty of confidentiality by persons acting on behalf of the Information Regulator; intentionally obstructing the execution of a warrant or, failing without a reasonable excuse to give assistance to a person executing a warrant; the responsible party providing a false statement, knowingly or recklessly when served with an information notice; and a witness failing to comply with lawful matters set out in section 104(1) of the POPIA.

[203] Section 107(a) of the POPIA.

[204] Section 107(b) of the POPIA.

[205] Section 109(1) of the POPIA.

[206] Section 109(2)(e) of the POPIA.

[207] Section 109(5) of the POPIA.

3.5 CONCLUDING REMARKS

In principle, the POPIA's enforcement and penalty regime is in line with the procedural or enforcement mechanisms identified by the SALRC, in that, the Act provides a system that provides support and assistance to data subjects to exercise their rights as well as adequate remedies where such rules have been violated. However, the SALRC's investigation was conducted before the rise of new and emerging technologies and the risks thereof to data privacy only surfaced much later. Therefore, the adequacy and effectiveness of the current POPIA enforcement and penalty regime has yet to be determined.

A recent survey revealed that, in implementing or enforcing the law, DPAs must have an understanding of the "information privacy implications of ICT used, large-scale analysis of personal data by a variety of interests, and emerging technologies such as emotion-detection and predictive data analytics."[209] Hence, a possible gap in ensuring effective enforcement of compliance with the POPIA lies in the fact that the Information Regulator may lack technical expertise to meaningfully detect or investigate the impact of existing and emerging technologies on data privacy. To strengthen the protection of data subjects, failure to effectively implement any of the lawful processing conditions should be regarded as a serious offence. Since section 40 (1)(b)(ii) and (e) of the POPIA requires that the Information Regulator take a proactive approach to address systemic issues before a breach occurs, the following chapter provides a deeper analysis of the envisaged execution of the Information Regulator's supervisory function to monitor technological developments.

[208] Ibid.
[209] C Raab and I Szekely 'Data Protection Authorities and Information Technology' (note 162 above) 421-33.

CHAPTER 4: AN ANALYSIS OF THE INFORMATION REGULATOR'S ROLE TO MONITOR THE ADVERSE EFFECTS OF TECHNOLOGICAL DEVELOPMENTS ON DATA PRIVACY

4.1 INTRODUCTION

In light of the advances brought about by the 4IR, governments face increasing pressure to change their approach to public engagement and policymaking. Legislators and regulators need to adapt to a new, fast-changing environment so they can truly understand what it is they are regulating.[210]

As discussed in Chapter 1, technological advancement has raised significant concerns relating to data subjects' data privacy.[211] This calls on DPAs to ensure robust foresight of the effect of new and emerging technologies on data protection in order to safeguard and advance data privacy rights and ensure effective enforcement of data protection laws.

This Chapter assesses the provisions of sections 40(1)(b)(ii)[212] and 40(e) of the POPIA that empower the Information Regulator to execute its functions.[213] Given that the POPIA is a new piece of legislation, the technological foresight[214] work conducted by well-established foreign DPAs in the UK and NZ is considered to determine if any lessons can be learnt from these jurisdictions.

4.2 FUNCTIONS OF THE INFORMATION REGULATOR

The fundamental role of DPAs includes eight key functions to advance the protection of personal information, namely, that of auditor; consultant; ombudsman; policy advisor;

---

210 Department of Telecommunications and Postal Services Concept Document: Establishment of the Presidential Commission on the Fourth Industrial Revolution in GN 764 *GG* 42078 of 4 December 2018.

211 See discussion in Chapter 1, paragraph 1.2.

212 See note 52 above.

213 See note 53 above.

214 DB Wills 'The technology foresight activities of European Union data protection authorities' (2017) 116 *Technological Forecasting & Social Change* 142 explains that activities involving technology foresight are "[c]entred around understanding new technology developments, and anticipating their potential effects and impacts and in the context of DPA's roles and their collaborative activity (where this activity is sometimes also termed 'technology watch') this focuses upon the potential impacts of emerging technologies upon data protection and privacy."

negotiator; educator; international ambassador and enforcer.[215] The POPIA includes all eight key functions; however, this discussion focusses on the role of the Information Regulator as educator, international ambassador, policy advisor and enforcer.

As educator, the Information Regulator must create awareness of the lawful processing conditions and objectives.[216] The Information Regulator's Outreach and Research Committee oversees research, public awareness, education and stakeholder management.[217] The Information Regulator confirmed that it has engaged with a number of organisations as part of an ongoing stakeholder and training programme in accordance with section 40 of the POPIA and that its focus area for its 2018/19 Annual Performance Plan included the development, approval and implementation of a Public Awareness Strategy.[218] This strategy should not be broad, but should specifically include, as a standing item, the recent types of technological developments which impact on data privacy risks so as to create awareness of the application of the lawful processing conditions when using a particular technology. However, the POPIA does not include a key provision on privacy by design and default[219] and it may thus be difficult to embed awareness of the use of new technologies to counter infringements of data privacy from the outset.

As policy advisor and enforcer, the Information Regulator must monitor and enforce compliance with the POPIA by *inter alia*, conducting research and monitoring developments in information processing and computer technology.[220] The term 'computer' should be removed from the technology monitoring function to avoid excluding other technologies and to ensure that it is broad enough to cover all forms of technologies used to process personal

---

[215] CJ Bennett 'The Data Protection Authority: Regulator, Ombudsman, Regulator or Campaigner?' Presentation at 24th International Conference of Data Protection and Privacy Commissioners 9-11 September 2002, available at *web.uvic.ca:8080/polisci/bennett/pdf/Cardiff.pdf* , accessed on 11 November 2019. See also SALRC Final Report (note 19 above) at 7.2.24.

[216] Section 40(1)(a)(i) of the POPIA.

[217] The Outreach and Research Committee is required to develop a Communications Policy and Strategy, Education and Public Awareness Strategy, Training Strategy and Plan, a Research Methodology with a prescribed and general focus and an Impact Assessment Strategy and Plan. See Information Regulator Terms of Reference "Outreach and Research Committee" available at *http://www.justice.gov.za/inforeg/docs/InfoRegSA-TOR-ORcommittee.pdf,* accessed on 20 September 2019.

[218] Information Regulator presentation on "Briefing of the Portfolio Committee on Justice and Correctional Services" dated 24 April 2018 available at *https://www.ellipsis.co.za/wp-content/uploads/2018/05/Information_Regulator_Briefing_24-April_2018.pdf,* accessed on 30 September 2019.

[219] This concept, also referred to as 'data protection by design and default', is discussed in Chapter 5, paragraph 5.2.2.6 below.

[220] Section 40(1)(b)(ii) of the POPIA.

information.[221] The Information Regulator is required to take legislative or other action to afford better protection to data subjects[222] and to report to Parliament on the adoption of necessary legislative amendments.[223] This is an important function which should be employed by the Information Regulator almost immediately to propose amendments to the POPIA to bring it in line with technological developments.[224] The role of policy advisor also extends to the Information Regulator being mandated to issue codes of conduct or guidelines for the development or application of codes of conduct.[225]

As international ambassador, the Information Regulator must co-operate with other persons and bodies concerned with data protection on a national and international basis. Importantly, the Information Regulator is entitled to research and report to Parliament on SA accepting any international instrument relating to the protection of personal information.[226]

As part of its 2018/19 Annual Performance Plan, one of the Information Regulator's focus areas was to develop a research strategy to address the "processing of personal information and computer technology that promote the protection of personal information and access to information."[227] No further status update on this strategy has been published by the Information Regulator; however, it is interesting that the research strategy focusses on privacy enhancing technologies (PETs)[228] rather than on technological developments which adversely impact data privacy protection as required by section 40(1)(e) of the POPIA.[229] For the Information Regulator to promote PETs, the POPIA will need to be amended to explicitly

---

[221] For instance, due to the impact of new or emerging digital technologies discussed in Chapter 1, paragraph 1.2 above, the current GDPR does not limit technological monitoring to computer technology and the proposed NZ Privacy Bill removes reference to the word 'computer' which is currently included in the NZ Privacy Act of 1993. See discussion under paragraphs 4.3.2.2 and 4.3.3.2 below.

[222] Section 40(1)(b)(iv) of the POPIA.

[223] Section 40(1)(e)(ii) of the POPIA.

[224] Refer to Chapter 5 for a discussion on law reform in other jurisdictions.

[225] Section 40(1)(f)(i) and (ii) of the POPIA.

[226] Section 40(1)(e)(i) of the POPIA.

[227] Information Regulator presentation on "Briefing of the Portfolio Committee on Justice and Correctional Services" dated 24 April 2018 available at *https://www.ellipsis.co.za/wp-content/uploads/2018/05/Information_Regulator_Briefing_24-April_2018.pdf* accessed on 30 September 2019.

[228] J Van den Hoven et al 'Privacy and Information Technology' (note 44 above) at 3.2, explains that privacy-enhancing technologies are tools which provide users with anonymity. These include, for example, communication-anonymising tools such as Tor and Freenet, which employ encryption methods as well as identity management systems such as 'single sign on' functions provided by Google, Facebook and Microsoft which allow users to use a single online identity to connect to various online services.

[229] As suggested, the word 'computer' should be removed from the technology monitoring function of the Information Regulator to avoid a situation where other technologies (which negatively impact data privacy) are excluded.

include privacy by design and default as a standard obligation for responsible parties, as is currently regulated by the GDPR.[230]

4.2.1. The Regulation of Technology-Specific or Technologically Neutral Data Protection

The regulation of data protection law is technologically neutral if the effect of the technology is regulated rather than the technology itself.[231] It has been argued that the objective of regulation of the function or effects of technologies is that the same regulatory principles should apply to both the online and offline environments without favour or discrimination.[232] However, the scope of application of a technologically-specific legal regime is limited to the regulation of specific technologies, which works well when there is a substantial difference between the functions or effects of different technologies.[233] Whilst the ECTA seeks to achieve a technologically-neutral approach to regulate electronic commerce transactions, it recognises the use of electronic signatures which is regarded as a technologically-specific form of regulation.[234]

Some authors state that, in the advent of rapid technological development, "technologically specific law is sometimes necessary to achieve technologically-neutral" regulation and that "any type of legislation is in fact technologically specific, since our environment is always technologically mediated."[235] However, technologically neutral data protection regulation is favoured by the OECD to embrace the changes in the technological and social environment.[236] Another view is that it may not be necessary for DPAs to research any new technologies due to the technological neutrality of data protection legislation in the

---

[230] Article 25 of the GDPR. See discussions under Chapter 5, para 5.2.3.6 below.

[231] B Koops 'The Trouble with European Union Data Protection law' (2014) 4(4) *International Data Privacy Law* 250-261. See further W Maxwell 'Technology neutrality in Internet, telecoms and data protection regulation' (2014) *Computer and Telecommunications L. Rev*, where the author explains that the concept of 'technology neutrality" means applying the same regulatory principles regardless of the technology used, and that law and regulations should not be drafted in technological silos.

[232] B Koops 'The Trouble with European Union Data Protection law' (note 231 above) 20.

[233] Ibid at 8, where the author accepts that "[t]echnology-specific regulation is acceptable only if there are material differences between technologies".

[234] Section 2(1)(f) of the ECTA.

[235] M Hildebrandt and L Tielemans 'Data Protection by Design and Technology Neutral Law' (2013) 19 *Computer Law & Security Review* 509-52 available at *http://www.sciencedirect.com/science/article/pii/S0267364913001313*, accessed on 2 September 2019.

[236] Organisation for Economic Co-operation and Development 'The Evolving Privacy Landscape: 30 Years After the OECD Guidelines*'* 06 April 2011 at 4-6 available at *https://www.oecd-ilibrary.org/the-evolving-privacy-landscape-30-years-after-the-oecd-privacy guidelines_5kgf09z90c31.pdf?itemId=%2Fcontent%2Fpaper%2F5kgf09z90c31-en&mimeType=pdf*, accessed on 25 November 2019.

EU. Nonetheless, it is acknowledged that due to the legal, moral and ethical constraints associated with new technologies, DPAs are key drivers to conduct the necessary research to understand their impact on data protection.[237]

The impact of technological changes on government, businesses and consumers is high on the agenda of SA's Presidential Committee on the Fourth Industrial Revolution, with data privacy cited as a key aspect which needs to be addressed.[238] In my view, a technologically neutral approach is the superior approach to regulate data protection as it does not prescribe the regulation of specific technologies. Technologically-specific regulation will be precarious given that other rapidly evolving or emerging technologies will not be regulated in fast-moving markets or that those that are regulated will become obsolete in a few years, necessitating an overhaul of the legislation. Instead, to keep pace with rapidly evolving technologies, the POPIA should contain a requirement that the Information Regulator conduct periodic reviews of the operation of this Act.

Furthermore, the Information Regulator should be proactive in developing binding codes of conduct or guidelines to address the specific use of technologies, which should also be reviewed or amended in line with sections 64[239] and 67[240] of the POPIA. For example, a code of conduct should be adopted for manufacturers of technologies[241] to ensure that privacy controls are embedded from the design stage (data protection by design and default).[242]

---

[237] DB Wills 'The technology foresight activities of European Union data protection authorities' (note 214 above) at 6.

[238] Speech Delivered by Communications Deputy Minister Pinky Kekana at the Microsoft Annual Digital Summit in Sun City on 23 May 2019 available at *https://www.doc.gov.za/speech-delivered-communications-deputy-minister-pinky-kekana-microsoft-annual-digital-summit-sun,* accessed on 30 September 2019.

[239] Section 64 (1) of the POPIA provides for the amendment or revocation of a code of conduct issued under section 60.

[240] Section 67 of the POPIA provides for the review of an approved code of conduct by the Information Regulator.

[241] M Hildebrandt and L Tielemans 'Data Protection by Design and Technology Neutral Law' (2013) (note 235), the authors argue convincingly that the data protection by design and default provision of the GDPR mainly targets data processors using technologies and not the designer or manufacturers of the technologies.

[242] See discussion in Chapter 5, paragraph 5.2.2.6 below.

4.3 TECHNOLOGY FORESIGHT ACTIVITIES OF DPAs: LESSONS FROM THE UNITED KINGDOM AND NEW ZEALAND

4.3.1 Overview

This section examines the statutory functions of DPAs in the well-established data protection regimes of the UK and NZ in order to draw lessons on how the Information Regulator should monitor technological developments to address data privacy concerns in line with international best practices. DPAs have been fully functional in these jurisdictions since the 1990s and practical insights into their technological foresight can be drawn that will add value to the work of the Information Regulator.

The discussion in this Chapter is limited to the statutory functions and activities undertaken by DPAs in the UK and NZ to monitor technological developments and to counteract adverse effects on data protection. The reforms adopted by these countries to enhance data privacy protection in the digital era are discussed in the following Chapter.

4.3.2 New Zealand

4.3.2.1 The Privacy Commissioner's Statutory Functions

The Privacy Act of 1993 ("the Privacy Act") governs data protection in NZ and establishes the NZ DPA as the Office of the Privacy Commissioner[243] ("the Commissioner"), which is an Independent Crown Entity.[244] The Commissioner functions independently from government or ministerial control. Section 13 of the Privacy Act sets out the functions of the Commissioner. For the purpose of this discussion, the functions contained in sections 13(1)(m) and (n) of the Act[245] are relevant to technological developments.

---

[243] The current Privacy Commissioner is Mr John Edwards. See the Office of the Privacy Commissioner's website available at *https://www.privacy.org.nz/the-privacy-act-and-codes/privacy-act-and-codes-introduction/*, accessed on 01 October 2019.

[244] Part 3, section 12 of the Privacy Act.

[245] Section 13(1)(m) of the Privacy Act provides that the Commissioner is empowered to "inquire about any enactment or law, practice, procedure, whether governmental or non-governmental, or any technical development if it appears that the privacy of an individual is being or may be infringed" and section 31(1)(n) of the Privacy Act mandates the Commissioner to "undertake research and monitor developments in data processing and computer technology by ensuring that adverse effects of such developments on the privacy are minimised and to report the results of such research and monitoring to the Minister responsible thereto."

The Commissioner's functions are similar to those of the Information Regulator in terms of the POPIA. The Commissioner is mandated to take proactive steps to research, monitor, advise, examine and report on any aspect which negatively impacts data privacy rights. In 2017, the Commissioner released a public statement on the privacy infringements caused by bulk disclosure of household level data recorded by smart meters which give rise to involuntary collection and device-based surveillance and is consequently regulated by the Privacy Act.[246] The Commissioner instructed electricity distributors using bulk smart meters to take certain steps to avoid the risks to data privacy order and infringement of data privacy rights.[247] The POPIA also allows the Information Regulator to make public statements on any matter affecting data protection.[248]

The Commissioner is empowered to issue codes of practice[249] aimed at modifying the privacy principles, which have the force of regulation and may be issued by the Commissioner itself or on application by a body representing any agency, profession, industry or calling.[250] For example, the Telecommunications Information Privacy Code[251] sets out rules on the deployment of caller line identification technology by a network operator. Other than this, the Commissioner has not issued a specific code of practice to regulate the use of any other form of new technologies used to process an individual's personal information.

The Privacy Act is undergoing amendment by means of the Privacy Bill which was introduced by the Minister of Justice on 20 March 2018. The Commissioner submitted extensive comments on the Law Commission's Review of the Privacy Act 1993: Stage 4.[252] With regard to the monitoring of technologies, the new Privacy Bill incorporates the Commissioner's comments in that reference to the word 'computer' in section 13(1)(n) was

---

[246] Privacy Commissioner's 'Public Statement about bulk disclosure of smart meter data', available at *https://www.privacy.org.nz/assets/Uploads/Open-letter-to-retailers-and-distributors-re-smart-meters-A504260.pdf*, accessed on 25 November 2019.

[247] Ibid.

[248] Section 40(1)(a)(iii) of the POPIA.

249 Section 46 of the Privacy Act. The Commissioner has since issued Codes of Practice which apply to the credit reporting, health and telecommunications sectors.

[250] Section 47 of the Privacy Act.

251 Telecommunications Information Privacy Code 2003 available at *https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/telecommunications-information-privacy-code/, accessed* on 09 October 2019.

[252] Refer to the discussion on the submissions made by the Commissioner in Chapter 5 at 5.4.2 below.

removed "since computers have become sufficiently ubiquitous as to need no reference and such reference" may have "the adverse effect of appearing to exclude other technologies."[253]

4.3.2.2 Monitoring Technological Developments

As part of its function to research and monitor technological developments, the Commissioner's current Technology Strategy[254] sets out the overarching strategic objectives of the Commissioner, which focus on priority outcomes to manage advancements in digital technologies. The Commissioner issues Statements of Intent every four years to achieve its strategic objectives.[255]

The Commissioner has a dedicated team to monitor technological developments and media reports. In researching and monitoring technological developments, the Commissioner undertakes activities such as releasing media statements on the use of technologies;[256] and participating in the work of the International Working Group on Data Protection and Telecommunications and the OECD Working Party on Information Security and Privacy. The Commissioner also conducts public opinion surveys on privacy and technological developments, and publishes 'getting started' guidelines, guidance notes,[257] information for

[253] Submission by the Office of the Privacy Commissioner on the Law Commission's Review of the Privacy Act 1993: Stage 4 dated 14 June 2010 at 82 available *https://privacy.org.nz/the-privacy-act-and-codes/privacy-law-reform/new-zealand-law-commission-privacy-review/*, accessed on 01 October 2019. See Chapter 5 for a discussion on the data protection law reform.

The Commissioner premised its strategy on technology work, focussing on the outcome of *'improved private sector privacy practices'*. The outcomes include creating good privacy practices by working with innovators to use privacy enhancing technology. See the Office of the Privacy Commissioner's Technology Strategy entitled 'Making the Future: Working with business to create a smarter, brighter future for privacy' dated December 2014 available at *https://www.privacy.org.nz/assets/Files/Policies-and-values-transparency/Making-the-Future-Working-with-business-to-create-a-smarter-brighter-future-for-privacy.pdf, accessed* on 02 October 2019.

255 In the latest Statement of Intent, the Privacy Commissioner will focus on digital technologies by increasing citizen/consumer trust in the digital economy, promote and support innovation and improve personal data practices by increasing influence. See Office of the Privacy Commissioner's Statement of Intention 2017-2021 available at *https://www.privacy.org.nz/assets/Uploads/OPC-Statement-of-Intent-2017-2022.pdf*, accessed on 02 October 2019.

256 For example, see media release: Meeting Technology Challenges Head On: Modern Tools for Modern Problems dated 2 August 2011 available at *https://www.privacy.org.nz/news-and-publications/statements-media-releases/media-release-meeting-technology-challenges-head-on-modern-tools-for-modern-problems/*, accessed on 02 October 2019.

257 Guidance Notes published on technological issues include cloud computing, CCTV and apps guidance. See Privacy Commissioner website link to guidance notes available at *https://privacy.org.nz/news-and-publications/guidance-resources/*, accessed on 03 October 2019.

agencies, blogs[258] and other educational resources on technological issues.[259] The Law Commission commended the Commissioner for raising awareness of new technologies, but highlighted that the Commissioner must provide guidance on new technologies at an earlier stage in order to assess the impact of these technologies on data privacy. The Law Commission thus proposed that the Commissioner should issue bulletins and updates on new technologies which should include developments or experiences from other countries.[260]

The Law Commission proposed that the Privacy Act provide for a Privacy Advisory Panel or that expert panels be set up by the Commissioner to address technological advances.[261] The Commissioner did not favour this proposal and submitted that a statutory committee should not be legislated but rather, the Commissioner should have the discretion to set up a panel of experts in line with its independence so that it can promptly respond to the dynamic privacy and technological environment in seeking external support and advice.[262]

4.3.3 United Kingdom

4.3.3.1 Overview

All countries in Europe are required to align their data protection laws to the EU GDPR[263] which took effect on 25 May 2018. The GDPR regulates the processing of personal data across every sector of the EU economy. The UK's Data Protection Act of 2018 ("DP Act") came into force on 23 May 2018, repealing the UK Data Protection Act 1998 in its entirety. The DP Act is designed to align to and supplement the GDPR data protection requirements.[264] The UK government described it as being "fit for the digital age."[265] The

---

[258] Blogs include information on big data. See Privacy Commissioner's website available at *https://privacy.org.nz/search/SearchForm?Search=big+data&Sections%5B1313%5D=1313&searchlocale=en_NZ&action_results=Go*, accessed on 03 October 2019.

259 See New Zealand Department of Internal Affairs website available at *https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/, accessed* on 02 October 2019 .

[260] Law Commission's Review of the Privacy Act 1993: Stage 4 (Report 123) (note 252) at paragraph 10.18.

[261] Ibid at paragraph 10.43.

[262] Submission by the Office of the Privacy Commissioner on the Law Commission's Review of the Privacy Act 1993: Stage 4 (note 253 above).

[263] *EU General Data Protection Regulation (GDPR):* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[264] William RM Long et al *The Privacy, Data Protection and Cybersecurity Law Review* 5ed (2018) 14.

GDPR has been described as better suited to the internet age as it creates rules for data protection for a Digital Single Market, thus giving individuals more control over their personal data.[266]

The use of cookies and similar technologies[267] is specifically regulated by the Privacy and Electronic Communications (EC Directive) Regulations (PECR) of 2003, which regulate the storage of information and access thereto on mobile or computer devices The European Directive 2002/58/EC ("the privacy Directive")[268] is implemented by the PECR. Specific protection from online privacy is necessary to enhance a data subject's rights and the POPIA is deficient in this regard.

4.3.3.2. The Information Commissioner's Office Statutory Functions

The Information Commissioner's Office (ICO)[269] is the UK's independent data supervisory authority which was established to uphold individual data privacy rights.[270] The ICO enforces both the DP Act and the PECR and is endowed with enforcement powers in terms of the GPDR to ensure compliance thereto.

---

265 See media publication of the *Department for Digital, Culture, Media & Sport* and *Home Office* available *at https://www.gov.uk/government/collections/data-protection-act-2018*, accessed on 02 October 2019.

266 A Giurgiu and TA Larsen 'Roles and Powers of National Data Protection Authorities: Moving from Directive 95/46/EC to the GDPR: Stronger and More "European" DPAs as Guardians of Consistency?' (2016) 2 *The European Data Protection Law Review* 347. See further A Giurgiu and G Lommel, 'A new Approach to EU Data Protection – More Control over Personal Data and Increased Responsibility' (2014) 1 *Critical Quarterly for Legislation and Law* 10-27, where the authors explain that the GDPR "[l]ays down solely the essential principles, thus avoiding becoming too detailed or too prescriptive. It puts a strong emphasis on placing the controller in a position where he needs to take responsibility for his actions. It also equips the data subjects with the proper tools to take control over their data and enforce their rights on- and off-line."

267 Similar technologies include fingerprinting techniques, scripts, tracking pixels and plugins. The forms of similar technological uses are described in detail in the ICO's "Guidance on the use of cookies and similar technologies" dated 03 July 2019, pages 6-7, available at *https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/, accessed* on 03 October 2019.

268 The Privacy Directive is more specific in terms of privacy rights in relation to electronic communications. According to the ICO, "it recognizes that widespread public access to digital mobile networks and the internet opens up new possibilities for businesses and users, but also new risks to their privacy." See ICO website for an overview of the PECR available at *https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/*, accessed on 02 October 2019. See also the ICO's "Guide to Privacy and Electronic Communications Regulations" available at *https://ico.org.uk/for-organisations/guide-to-pecr/*, accessed on 02 October 2019. See further discussion in Chapter 5, paragraph 5.2.1 below.

269 Elizabeth Denham is the current Information Commissioner of the ICO.

270 Section 115(1) of the DP Act.

Part 5 of the DP Act read with Schedules 12 and 13[271] sets out the ICO's powers, functions and duties. General functions are conferred on the ICO by Articles 57 (tasks) and 58 (powers) of the GDPR. Schedule 13 of the DP Act also includes certain general tasks conferred on the ICO in terms of Article 57 of the GDPR. The relevant general tasks of the ICO set out in Schedule 13[272] to ensure that the processing of personal information is not negatively impacted by technological developments include monitoring relevant technological developments,[273] promoting public awareness of the risks associated with processing personal data[274] and advising Parliament, government or institutions on relevant legislative or administrative measures to enhance personal data protection.[275]

4.3.2.3 Monitoring Technological Activities

Like the NZ Commissioner, the ICO published a Technology Strategy[276] aligned to its Information Rights Strategic Plan 2017-2021 to "[s]tay relevant, provide excellent public service and keep abreast of evolving technology" and to "outline the means of adapting to technological change as it impacts information rights ..... to plan ahead for the arrival of new technologies…."[277] The ICO acknowledges that technological advances and data privacy and innovation are not mutually exclusive, but operate hand-in-hand to create trust and confidence and must be viewed as a risk and an opportunity.[278] The Technology Strategy sets out eight technology goals and the manner in which these will be achieved.[279] In addition, the ICO's Innovation Plan[280] addresses the manner in which new technologies or disruptive business models could adapt to the UK's legislative and enforcement framework and how new technologies can shape regulated sectors.

---

[271] In terms of section 116(2) of the DP Act, "Schedule 13 confers general functions on the Commissioner in connection with processing to which the GDPR does not apply."

[272] Schedule 13 of the DP Act contains a repetition of some of the tasks assigned to the supervisory authorities in terms of Article 57 of the GDPR because the legislature intended that key functions should remain vested in the ICO even after the UK exits the EU.

[273] Schedule 13(1)(h) of the DP Act. The GDPR contains similar wording to this provision; however, it expands application to "commercial practices". See Article 57 of the GDPR.

[274] Schedule 13 (1)(b) of the DP Act.

[275] Schedule 13 (1)(c) of the DP Act.

276 Information Commissioner's Office 'Technology Strategy 2018-2021' available at *https://ico.org.uk/media/about-the-ico/documents/2258299/ico-technology-strategy-2018-2021.pdf,* accessed on 2 October 2019.

[277] Ibid at 4.

[278] Ibid at 3.

[279] See Information Commissioner's Office 'Technology Strategy 2018-2021' (note 276 above).

280 Information Commissioner's Office "Innovation Plan" dated April 2017 available at *http://www.gov.uk/government/publications/ico-innovation-plan,* accessed on 02 October 2019.

The ICO's technology foresight activities are based on a "intelligence hub" that gathers information and intelligence from various sources, such as academics, journalists and technologists.[281] Recent planned technological foresight activities or initiatives undertaken by the ICO include the following:-

(i) participation as an active member in international forums on technology;[282]

(ii) a Technology Reference Panel was formed, with expert consultants soliciting advice on the technological issues impacting data protection;[283]

(iii) An ICO Technology Policy Department which focusses on horizon scanning for new technological developments;

(iv) publication of various guidance documents on technologies to apply the data protection principles;[284]

(v) providing guidance and advice to industry regarding the 'privacy by design' approach[285] and the use of the Privacy Impact Assessment code of practice;[286]

(vi) commissioning internal research on the impact of new technologies relating to personal data;[287]

(vii) blogs on technology and innovation and guidance on privacy impact assessments are published on the ICO's website;[288]

---

[281] D Barnard-Wills 'The technology foresight activities of European Union data protection authorities' *Technological Forecasting & Social Change* (2016) 4.

[282]The ICO regards engagement with external stakeholders on identifying trends or developments of technology as 'open policy development'. The ICO is a member of the Working Party 29 Technology Subgroup, International Working Group on Data Protection in Telecommunications; and the Internet Privacy Engineering Network. See ICO's Innovation Plan (note 280 above).

[283]Ibid.

284 Guidance documents have been published on artificial intelligence, data protection, cloud computing, big data, encryption, machine learning, Wi-Fi location analytics and cookies and similar technologies. See ICO website "Guidance Index" available at *https://ico.org.uk/for-organisations/guidance-index/data-protection-act-1998/*, accessed on 02 October 2019.

[285]The ICO recently launched the Sandbox service to support organisations to develop products and services that use personal data in an innovative and compliant manner. See ICO website "The Guide to the Sandbox (beta phase)" available at *https://ico.org.uk/for-organisations/the-guide-to-the-sandbox-beta-phase/*, accessed on 05 October 2019.

[286]Information Commissioner's Innovation Plan (note 280 above).

[287]Research is being conducted on artificial intelligence, the Internet of Things and automated decision making, big data and remotely piloted aircraft systems or drones. See Information Commissioner's Innovation Plan (note 280 above).

(viii) setting up an ICO Grants Programme to promote research into innovative solutions relating to technologies such as machine learning and artificial intelligence.[289]

The ICO was consulted by the court in *R v The Chief Constable of South Wales Police and others*.[290] Whilst the court ruled that the use of live facial recognition technology was lawful when conducted by the police for investigation purposes, it acknowledged that legislative steps should be taken to keep pace with such technology. In light of this recommendation, the ICO, suggested that "a statutory and binding code of practice…..should seek to address the specific issues arising from police use of live facial recognition technology and other biometric technologies."[291]

Furthermore, in response to developments in surveillance technologies, the ICO revised its CCTV code of practice[292] and more recently tabled the Data Sharing Code to the Secretary of State for approval.[293] A recent write-up highlighted that UK businesses are ramping up compliance with the GDPR and are proactively reporting personal data breaches to the ICO.[294]

4.4 CONCLUDING REMARKS

Echoing the sentiments expressed by the South African government in the introductory paragraph of this Chapter and authors such as Flaherty who are of the view that "[o]ne cannot regulate a system without fully understanding it," DPAs' expert knowledge plays an important role in this regard.[295] It has been argued that their role of monitoring technological

---

288 See ICO website "Tech and Innovation" available at *https://ico.org.uk/about-the-ico/what-we-do/tech-and-innovation/,* accessed on 05 October 2019.

[289] Ibid.

[290] [2019] EWHC 2341.

[291] ICO's 'Opinion on the use of live facial recognition technology by law enforcement in public places' 31 October 2019 available at *https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf,* accessed on 25 November 2019.

292 ICO 'CCTV Codes of Practice' available at *https://ico.org.uk/media/1542/cctv-code-of-practice.pdf*, accessed on 25 November 2019.

293 ICO 'Data Sharing Code' available at *https://ico.org.uk/media/2615361/data-sharing-code-for-public-consultation.pdf,* accessed on 02 November 2019.

294 Reed Smith 'One year of GDPR – lessons learned by the ICO' 4 June 2019, available at *https://www.technologylawdispatch.com/2019/06/privacy-data-protection/one-year-of-gdpr-lessons-learned-by-the-ico/,* accessed on 27 November 2019.

[295] D Flaherty 'Controlling Surveillance: Can Privacy Protection Be Made Effective?' (2018) in Agre, P. and Rotenberg, M. (eds.) *Technology and Privacy: The New Landscape.* Cambridge, MA: The MIT Press: 167-192. See also C Raab and I Szekely 'Data Protection Authorities and Information Technology' (note 162 above) 421–33.

developments requires ICT expertise as they need to keep abreast of the impact of new technologies on data privacy. I support the view that the "excessively 'legal' image of DPAs should be corrected."[296]

The technological foresight activities of the UK and NZ's DPAs demonstrate that the Information Regulator should adopt a proactive rather than a reactive stance in undertaking technological foresight. Given that the Information Regulator is assuming a new role as a data protection regulator, it may not be fully resourced with the technical skills and ICT expertise required to fully carry out the technological foresight activities conducted by the UK and NZ DPAs.

Therefore, as a short to medium term goal, the Information Regulator should adopt the ICO's "intelligence hub" model by gathering information and intelligence from various sources, such as academics, journalists and technologists and also amend the POPIA to include data protection by design and default requirements to strengthen its technological monitoring role. In the long term, the Information Regulator may elect to adopt the recommendation of the NZ Commissioner and establish an expert panel for external support and advice.

[296] C Raab and I Szekely 'Data Protection Authorities and Information Technology' (note 162 above) 421–33.

CHAPTER 5: DATA PROTECTION LAW REFORM IN THE EUROPEAN UNION, UNITED KINGDOM AND NEW ZEALAND

5.1 INTRODUCTION

It is clear that on-going technological developments have increased the risk of privacy infringements.[297] As discussed in Chapter 4, DPAs have a statutory duty to monitor the impact of technologies and to propose updates to their respective data protection legal regimes to ensure that such laws keep pace with rapid advances in technology.

Whilst not all features of foreign data protection legal reform may be relevant to SA, the POPIA needs to remain adequate to achieve the objective of protecting the individual's right to privacy in an ever-changing technological era. The features of legal reform in the data protection regimes of the EU, the UK and NZ are considered in this Chapter to determine the extent to which such legal reform may promote data privacy protection in the South African context, in terms of enhancing the protection afforded to data subjects to counter the negative impact of new or emerging technologies on data privacy.

5.2 REFORM OF THE EU DATA PROTECTION REGIME

5.2.1 Background

Globally, the EU has led legal and policy formulation for data protection and the POPIA was largely premised on the earlier EU data protection legal instruments and guidelines.[298] It has been noted that, in terms of the Bill of Rights, the courts have an obligation to consider international law;[299] therefore any defining feature of legal developments with specific regard to legislative reform influenced by technological changes adopted by foreign jurisdictions should be considered by the Information Regulator to provide better data privacy protection.

---

[297] Refer to Chapter 1, paragraph 1.2 above for a discussion on new and emerging communications and information technologies which pose data protection challenges.

[298] SALRC Final Report (note 19 above) 163-4. The legislature adopted the OECD Guidelines and the EU Directive data protection principles. The SALRC stated that these data protection principles are internationally accepted best practices and also technologically neutral.

[299] Y Burns and A Burger-Smidt *A Commentary on the Protection of Personal Information Act* (note 68 above) 8.

The EU recognises data protection as a separate right to the right to privacy.[300] Following a proposal by the European Commission (EC) to address inconsistencies in member states' data protection law, the EU Directive[301] was adopted as an omnibus data protection regime.[302] While it required member states to enact data protection legislation, the harmonisation of national data protection laws was not fully achieved as member states favoured big tech companies by imposing weak enforcement penalties. Coupled with the explosion in internet users, this prompted the EC to set the wheels in motion to propose legislative reform to modernise and replace the provisions of the EU Directive.

The courts interpret EU legislation together with interpretation by the European Data Protection Board, whose opinions have persuasive and non-binding force. If national judges have difficulty interpreting EU rules, they may, in some cases, refer the matter to the Court of Justice of the European Union (CJEU).[303] The CJEU is the highest authority which deals with interpretation of EU data protection laws.[304] For example, it granted data subjects a 'right to be forgotten'[305] and recently ruled that active consent is required for the storage of cookies which are used to track online browsing behaviour.[306]

May 2018 witnessed a regulatory paradigm shift in the EU data protection regime consisting of a legal reform package in the form of the GDPR[307] and the Law Enforcement Directive.[308] The GDPR repealed the 1995 EU Directive in its entirety.[309] This Regulation

---

[300] Article 7 of the Charter of Fundamental Rights of the European Union.

[301] 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.

[302] CJ Hoofnagle et al 'The European Union general data protection regulation: what it is and what it means?' (2019) 28(1) *Information & Communications Technology Law* 65-98 available at *https://www.tandfonline.com/doi/citedby/10.1080/13600834.2019.1573501?scroll=top&needAccess=true,* accessed on 29 September 2019.

[303] Article 19(3)(b) of the Treaty on European Union.

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

305 Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos* (May 13, 2014) available at *http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN,* accessed on 01 October 2019.

[306] L. Mitrou "Data Protection, Artificial Intelligence and Cognitive Services: Is The General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" December 2013 available at *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914,* accessed on 31 July 2019.

307 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 (General Data Protection Regulation) available at *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, accessed* on 30 July 2019. The GDPR entered into force on 24 May 2016 and was effective as of 25 May 2018.

[308] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,

aims to enhance the protection of data privacy in the digital age and to set rules for data processors in the digital single market. Overall, the GDPR harmonises data protection law across the EU to maintain consistency in the legal systems of member states and to prevent unnecessary administrative burdens.[310] Importantly, it takes particular cognisance of rapid technological developments which rendered the 1995 EU Directive inadequate in providing a high degree of protection of data privacy.[311] The ePrivacy Directive which regulates online privacy in the EU is also in the process of undergoing amendments through a proposed ePrivacy Regulation.[312]

Since data privacy is a moving target that is impacted by technological developments, it is necessary to ensure that a data protection legal regime is fine tuned to address deficiencies through legislative reform. However, it is yet to be seen if the enhanced protection afforded by the GDPR can withstand the new or emerging technologies used to process personal data.

5.2.2 Changes to the EU Data Protection Regime

The GDPR is technologically neutral in that it affords protection to a data subject[313] irrespective of the form or type of technology used to process personal data.[314] It has been described as "technology-independent legislation" which does not refer to "technology-specific terminology but the provisions thereof exhibit a 'technological neutrality approach'."[315] The discussion below does not present a detailed analysis of all changes to the EU data protection regime, but focusses on the novelty provisions of the GDPR

---

and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA available at *https://eur-lex.europa.eu/legal content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC* ,accessed on 30 July 2019. The Enforcement Directive was passed on 5 May 2016 and came into effect on 6 May 2018.

[309] See Article 94(1) of the GDPR. The EU Directive required EU member states to transpose its provisions into their national laws; however, the GDPR, as a regulation, takes direct effect on EU member states, meaning that, they do not have to transpose the provisions of the GDPR into their national laws. However, the GDPR allows member states to derogate from certain provisions in their national laws. Article 23 allows member states to derogate from certain provisions of the GDPR relating to rights in Articles 12 to 22 and from the data protection principles in Article 5 provided that they correspond to the rights in Articles 12 to 22.

[310] Recital 9 of the preamble of the GDPR.

[311] Recital 6 of the preamble of the GDPR.

[312] See discussion under paragraph 5.2.2.7 below.

[313] The GDPR does not contain a separate definition of a 'data subject' but encompasses the description of a data subject in the definition of 'personal data'. See Article 4(1) of the GDPR.
Unlike the POPIA, the GDPR does not recognise a juristic person as a data a subject.

[314] Recital 15 of the Preamble of the GDPR.

[315] Ibid.

encompassing enhanced rights to data subjects and obligations imposed on data controllers[316] to prevent data privacy infringement occasioned by the use of technology. These provisions are not specifically addressed by the POPIA. The novelty provisions discussed below prescribe the manner in which personal data can be processed by new or emerging technologies.

5.2.2.1 Definitions

The GDPR applies to any data which identifies or could identify an individual, directly[317] or indirectly,[318] including public and non-sensitive information.[319] The wide application of the GDPR in a 'smart environment' has created the perception that the GDPR requirements will, in future, apply to all forms of data, becoming 'the law of everything'.[320] The definition of 'personal data' extends to the 'online identifier' and 'location data',[321] which is aligned to the online reality. For example, the GDPR obligations will apply where a device is linked to an IP address because such address can be indirectly linked to the identity of an internet user.[322]

With reference to Recital 26 of the GDPR, Mitrou states that, although vague, identifiability is a dynamic criterion which takes into account the technology used at the time of processing as well as technological advances.[323] Hence, notwithstanding the technology used, identifiability is triggered by singling out the identity of the data subject, whether

---

316 A 'controller' is defined in the GDPR as "[t]he natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law." See Article 4(7) of the GDPR.

317 This includes obvious data applicable to a natural person such his or her name, identity number, addresses or contact details. See the EU GDPR website available at *https://gdpr.eu/eu-gdpr-personal-data/*, accessed on 07 December 2019.

318 It includes less obvious data such as online identifiers, location data, or factors relating to the physiological, physical, mental, genetic, social, cultural or economic identity of a natural person. See the EU GDPR website available at *https://gdpr.eu/eu-gdpr-personal-data/*, accessed on 07 December 2019.

319 CJ Hoofnagle et al 'The European Union general data protection regulation: what it is and what it means?' *Information & Communications Technology Law* (note 302 above).

320 N Purtov 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) *Law, Innovation and Technology* 40 available at *https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176*, accessed on 30 September 2019.

321 Recital 30 of the GDPR. See further L Mitrou 'The General Data Protection Regulation: A Law for the Digital Age?' (note 133 above) 24.

322 Ibid 24. Also see Case C-582/14 *Breyer v Bundesrepublik Deutschland* ECLI:EU:C:2016:779 at 35, where the European Court of Justice broadly interpreted the 1995 EU Directive to include an IP address stored by an internet service provider as personal data, which "registers IP addresses of the users of a website that it makes accessible to the public, without having the additional data necessary in order to identify those users."

directly or indirectly.[324] For example, data such as the name, email address, biometric data, facial recognition, location, preference or search history fall within the ambit of personal data.

Furthermore, the term 'processing' is expanded in the GDPR.[325] Technologies such as Blockchain and Artificial Intelligence or machine learning which are automated means that perform operations relating to personal data, continued storage thereof and/or further processing, fall squarely within Article 4(2) of the GDPR.

5.2.2.2 Extraterritorial Application

The GDPR has extraterritorial application,[326] which means that it can apply even if a business has no physical presence in the EU.[327] The European Court of Justice (ECJ) set out the factors to be considered when determining the territorial scope of EU data protection law.[328] The GDPR will apply exterritorialy if two conditions are met, namely, where processing activities relate to the "offering of goods or services, irrespective of whether a payment of the data subject is required to such data subjects in the Union"[329] and "where processing activities relates to the monitoring of behaviour as far as this behaviour takes place within the Union."[330] This means that South African businesses must comply with the GDPR if they trigger the activities stated in Articles 3(2)(a) and (b) of the GDPR.

---

[323] L. Mitrou "Data Protection, Artificial Intelligence and Cognitive Services: Is The General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" (note 306 above) 30.

[324] Recital 26 of the GDPR.

[325] Article 4(2) of the GDPR.

[326] Article 3(1) of the GDPR.

[327] See for example, Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, where the Court held that Google Spain is an establishment of Google Inc., and the selling of advertising activities was "carried out in the context of the activities of the Spanish establishment, so the search engine had to comply with EU law."

[328] C-230/14, *Weltimmo S.R.O. V. Nemzeti A Datvedelmi Es Informacioszabadsagh Atosag (Hungarian DPA*), 1.10.15. The ECJ decided that factors such as "the degree of stability of the arrangements and the effective exercise of activities … must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned."

[329] Article 3(2)(a) of the GDPR. See the European Parliament's study on the 'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?' (note 344 above) where the example is used of blockchain operators that offer infrastructure as a service to individuals in the EU.

[330] Article 3(2)(b) of the GDPR. See the European Parliament's study on the 'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?' (note 344 above) where it was illustrated that the GDPR will apply where foreigners use blockchain technology to process personal data to monitor the behaviour of individuals based in the EU.

The fact that the GDPR is described as "international data protection law,"[331] has raised contention as there could be a conflict between the EU data protection legislation and that of countries outside the EU.[332] Ambiguity in this regard has been justified by the fact that non-EU business will have to comply with the GDPR if they offer goods or services to EU citizens or if they monitor the behaviour of such citizens. It such cases, the GDPR requires businesses to appoint representatives located within the EU or in the specific member state.
[333]

5.2.2.3 Lawfulness of Processing in Terms of Consent

As a starting point in proposing legislative amendments, the EC emphasised the need for more effective control of personal information in the digital era. Consent is arguably the most fundamental safeguard afforded to data subjects to exercise their rights to informational self-determination.[334] As a new formulation under the GDPR, consent involves a restrictive approach in that it must be "freely given, specific, informed and unambiguous."[335]

A request for consent by electronic means must be "clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."[336] For example, pre-tick boxes, silence or inactivity do not constitute consent. The CJEU recently delivered judgment in the Planet49[337] case which dealt with the requirements of consent for the use of cookies and similar technologies. The court had to decide whether pre-ticked boxes on an online lottery service which allowed users to opt out of the use of cookies satisfied the

---

[331] S Bu-Pasha 'Cross-border issues under EU data protection law with regards to personal data protection' (2017) 26 (3) *Information & Communications Technology Law*) 213-228.
[332] Ryngaert, C & Taylor, M 'Symposium on the GDPR and International Law: The GDPR as Global Data Protection Regulation?' (2020) available at *https://www.cambridge.org/core/services/aop-cambridge-core/content/view/CB416FF11457C21B02C0D1DA7BE8E688/S2398772319000801a.pdf/gdpr_as_global_data_protection_regulation.pdf*, *accessed* on 02 January 2020, where it is explained that EU data protection law is based on territoriality, triggered by a territorial link of an activity or person residing in the EU or those being targeted or monitored in the EU. The GDPR's broad territorial coverage also applies to individuals who are able to demonstrate an affiliation to the EU, either by citizenship or residence. The authors indicated that the assertions of the EU that the GDPR has extraterritorial application "may be justifiable under the passive personality principle, which allows the EU to protect EU citizens or residents…."
[333] Article 27 and Recital 80 of the GDPR. See further Bu-Pasha, S. 'Cross-border issues under EU data protection law with regards to personal data protection' (note 331) 219.
[334] L Mitrou 'The General Data Protection Regulation: A Law for the Digital Age?' (note 133 above) 34.
[335] See definition of 'consent' in Article 4(11) of the GDPR and see further Recital 32 of the Preamble to the GDPR.
[336] Recital 32 of the GDPR.
[337] *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband* eV, Case C-673/17 ECLI:EU:C:2019:246.

requirements of specific and unambiguous consent. The CJEU held that such boxes are not valid because this does not provide affirmative consent as required by the ePrivacy Directive, the 1995 EU Directive and, now the GDPR, and stated as follows:

> In that regard, it would appear impossible in practice to ascertain objectively whether a website user had actually given his or her consent to the processing of his or her personal data by not deselecting a pre-ticked checkbox nor, in any event, whether that consent had been informed.[338]

For consent to be informed, the data subject must be aware of the purpose of the processing of the personal data as well as the identity of the controller.[339] Another unique feature of the GDPR is that the onus is on the controller to demonstrate that the data subject has consented to the processing of his or her personal information.[340] The Article 29 Data Protection Working Party has issued 'Guidelines on Consent' to clarify the scope of its application.[341] It is recommended that mechanisms to comply with the consent requirements under the GDPR should include written acknowledgment by the data subject such as clicking an 'I-agree-button' together with a privacy policy.[342]

5.2.2.4 Right to be Forgotten

The right to be forgotten embraces informational self-determination that enables data subjects to exercise control over their personal information. The GDPR allows data subjects to obtain 'erasure' of their personal data from the data controller subject to certain conditions.[343] The right of erasure has been described as "a qualified and a limited right."[344] In the *Peter Nowak*

[338] Ibid at paragraph 55.
[339] Recital 42 of the GDPR.
[340] Article 7(1) of the GDPR.
[341] Article 29 Data Protection Working Party "Guidelines on consent under Regulation 2016/679" WP259rev.01, 10 April 2018 18 available at *https://webcache.googleusercontent.com/search?q=cache:l-b4dUk35iAJ:https://ec.europa.eu/newsroom/article29/document.cfm%3Faction%3Ddisplay%26doc_id%3D51030+&cd=1&hl=en&ct=clnk&gl=za,* accessed on 09 November 2019.
342 T Mulder 'Health Apps, their Privacy Policies and the GDPR' (2019) 10 (1) *European Journal of Law and Technology* 7 available at *http://ejlt.org/article/view/667/897,* accessed on 09 November 2019.
[343] Article 17(1) of the GDPR.
[344] The European Parliament's study on the 'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?' (note 344 above) 75. See also Case C-398/15 *Salvatore Manni* [2017] EU:C: 2017:197 at 46 where court recognised that the right of erasure of data is guaranteed in instances where the conditions laid down in the then 1995 EU Directive were not complied with by the data controller.

case the ECJ held that the right to erasure cannot be invoked for the purposes of correcting incorrect examination results as this counters the spirit of Article 17 of the GDPR.[345]

The leading case on the right to be forgotten is *Google v Spain*,[346] where the CJEU held that the 1995 EU Directive authorises a data subject to demand that the search engine operator remove personal information containing his or her name from search results and links to web pages published by third parties "on the ground that . . . he wishes it to be 'forgotten' after a certain time."[347] However, the court indicated that this right is not absolute. The court then turned to right to be forgotten in terms of the GDPR and also held that this right is not absolute on the basis that Google could refuse the data subject's request if any of the conditions contained in Article 17(3) of the GDPR apply.[348]

Recently, in *Google v CNIL & Others*[349] the CJEU dealt with the interpretation of the territorial scope of the right to be forgotten contained in Article 17 of the GDPR and considered whether Google is required to carry out de-referencing on all search engines worldwide or merely on those provided in the EU. It was held that the right to be forgotten does not have global application. Whilst the Court acknowledged that the internet has no borders, it stated that the obligation to de-reference for versions of search engines outside the EU does not exist under EU data protection legislation.

5.2.2.5 Right to Data Portability

An innovative feature of the GDPR is the right to data portability which allows the data subject to transfer or port data from one controller to another.[350] The right to data portability can be relied on only if certain conditions are met, namely, the data subject provided the

[345] Case C-434/16 *Peter Nowak* [2017] EU:C: 2017:994 at 52.

[346] Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (note 327).

[347] Ibid at paragraph 89.

[348] These conditions include exercising the right of freedom of expression and information, to comply with a legal obligation where processing by the controller is required for the performance of a task carried out in the public interest or in the exercise of official authority, for reasons of public interest regarding public health; for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; and for the establishment, exercise or defence of legal claims.

[349] C-507/17, *Google v. CNIL* and *C-136/17, G.C. and Others v. CNIL.*

[350] Article 20 of the GDPR. See also Article 29 Data Protection Working Party "Guidelines on the Right to Portability" (2017*)*, WP 16/EN, WP 242 rev.01, 4.

personal data to the data controller,[351] the processing is based on consent or contract,[352] and the processing is executed through automated means.[353] If the request for portability complies with these conditions, data controllers must ensure that the data is made available to the data subject in a "structured, commonly used and machine-readable format."[354]

5.2.2.6 Data Protection by Design and Default

The concept of privacy by design means that the design, development or creation of new technologies must incorporate data privacy protection from the outset of the design of ICT processing systems. The ICO stated that the GDPR now codifies privacy by design which was previously a good practice measure under the 1995 EU Directive.[355] Privacy by design is a valuable innovative obligation in the GDPR which is a preventative measure to enhance data privacy protection by ensuring that technologies used to process personal data are designed to incorporate controls to mitigate the risks of unlawful processing. This precautionary approach aims to deal with the challenges posed by new technologies and adapts data protection law to technological developments.[356]

Article 25 of the GDPR obliges data controllers to implement appropriate technical and organisational measures to give effect to the data protection principles as well as to integrate safeguards into the processing to comply with the requirements of the GDPR, thereby protecting the rights of the data subject. However, Bygrave identifies certain flaws in Article 25 including vagueness, the complexity of the language used, the failure of the provision to clarify parameters and methods to achieve compliance, the lack of strong incentives to abide

[351] Article 20(1) of the GDPR.
[352] Article 20(1)(a) of the GDPR.
[353] Article 20(1)(b) of the GDPR.
[354] Article 20(1) of the GDPR. See further Article 29 Data Protection Working Party 'Guidelines on the right to data portability' 6/EN WP 242 rev.01 adopted on 13 December 2016 available at *https://iapp.org/media/pdf/resource_center/WP29-2017-04-data-portability-guidance.pdf*, accessed on 12 September 2019, where it was explained that the notion of data portability "empowers data subjects to move, copy or transmit personal data easily from one IT environment to another."
355 ICO 'Data protection by design and default' available at *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/*, accessed on 10 November 2019.
[356] L. Mitrou "Data Protection, Artificial Intelligence and Cognitive Services: Is The General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" (note 306 above) 76.

by its requirements and failure to communicate with the engineers who design and develop information systems.[357]

Encryption is an example of data protection by design, which encodes messages to be accessible by authorised users only. An example of data protection by default is the creation of privacy-friendly settings on social media networks which limit the accessibility of user profiles so that they cannot be accessed, by default, by an indefinite number of natural persons. Proof of compliance with the requirements of Article 25 is linked to the certification mechanisms provided for in Article 42 of the GDPR.[358]

5.2.2.7 Regulation of Online Privacy

The current ePrivacy Directive in the EU, which only applies to personal data processed in relation to electronic communications services in public communication networks, provides a greater degree of data privacy, regardless of the type of technology used. For instance, the ePrivacy Directive requires EU member states to ensure that consent is obtained from a user before cookies can be stored or accessed from his or her smartphone, computer or any other device connected to the internet. It also applies to tracking technology and direct marketing. In January 2017, the EC issued a proposal for an ePrivacy Regulation[359] which aims to replace the ePrivacy Directive and to complement the GDPR. The POPIA, in its current form, does not deal with online privacy and there is no specific legislation in SA dealing with such.

5.3 UNITED KINGDOM

5.3.1 Background

The DPA largely codifies the GDPR into UK law but contains allowable derogations in accordance with the GDPR. Part 2, Chapter 2 of the DPA contains the derogations from the

[357] LA Bygrave 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4 *Oslo Law Review* 11.

[358] Article 42 of the GDPR encourages data controllers to establish certification mechanisms such as data protection seals and marks.

[359] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD) available at

GDPR which supplement the GDPR, whilst Part 2, Chapter 3 contains applied GDPR provisions. Therefore, key differences between the DPA and the GDPR were enacted in contemplation of the British Government's exit ("Brexit") from the EU. The DPA was developed to maintain the GDPR data protection regime post the UK's exit.[360] The UK exited the EU on 31 January 2020.[361] In terms of the Withdrawal Agreement and Political Declaration[362] agreed to between the EU and the UK following the latter's exit, unless extended, a transition phase runs up to 31 December 2020[363] during which time EU law, including the GDPR will remain applicable to the UK. The UK courts will continue to apply the CJEU's decisions and any amendments to EU law during the transition phase. Basically during the transition phase, the UK will continue to function as an EU member state without restriction on data transfers and the ICO will remain a supervisory authority.

5.3.2 The UK Data Protection Regime

After the GDPR came into force in all EU member states with effect from 25 May 2018, the UK Government elected to pass the DPA in 2018, which contains derogations, adaptations and exemptions from the GDPR.[364] As a third generation data protection statute, the DPA repealed the Data Protection Act of 1998 in its entirety.[365] The DPA governs the processing of personal data relating to individuals by public and private bodies, intelligence services and law enforcement authorities and is enforced by the ICO as the national supervisory authority.[366]

---

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010, accessed on 2 December 2019.

[360] European Union (Withdrawal) Act 2018 available at *http://www.legislation.gov.uk/ukpga/2018/16/contents/enacted*, *accessed* on 04 November 2019.

361 See the UK Government's website available at *https://www.gov.uk/brexit*, accessed on 16 November 2019.

[362] On 17 October 2019, the UK and the European Council reached an agreement on the UK's withdrawal from the EU. The Withdrawal Agreement will need to be ratified by the EU and the UK before it can enter into force.
The revised Withdrawal Agreement and Political Declaration is available at *https://www.gov.uk/government/publications/new-withdrawal-agreement-and-political-declaration,* accessed on 15 November 2019.

[363] Article 126 of the Revised Withdrawal Agreement. Ibid at 186.

364 Mc Cullagh et al 'National Adaptations of the GDPR' (2019) *Collection Open Access Book* available at *https://wp.me/p6OBGR-3dP,* accessed on 04 November 2019.

[365] Schedule 19, paragraph 44 of the DPA.

[366] Part 1 section 1 of the DPA.

Part 2, Chapter 2 together with Schedules 1 to 3 of the DPA contain the derogations allowed by the GDPR.[367] With a specific focus on the digital environment, the DPA contains the following key derogations from the GDPR:-

5.3.2.1 Child's consent[368]

The GDPR requires that a child of 16 should consent to data processing for the purposes of the provision of information society services (ISS), whilst the DPA sets the age at 13. The explanatory note to the DPA 2018 clarifies that this derogation is "in line with the minimum age set by Facebook, WhatsApp and Instagram."[369] On 12 April 2019, the ICO drafted and released a 'Code of Practice for Age appropriate design' for comment which targets online services and provides guidelines for the design standards for ISS when processing personal data that will likely be accessed by children.[370] McCullagh argues that this Code of Practice is likely to pose challenges for ISS in setting up parental consent mechanisms to demonstrate that they implemented appropriate technical measures to verify a child's age, which may prove difficult considering that children could employ techniques to bypass the parent consent verification mechanisms.[371]

5.3.2.2. Definition of 'identifier'

The GDPR has a more detailed and expansive meaning of 'identifier' in the definition of personal data than the DPA. The GDPR makes it clearer that personal data extends to an online identifier such as IP addresses and cookies, which reflects technological changes in the processing or collection of personal information. The DPA merely includes reference to an 'online identifier' in the term 'identifiable living individual' without expanding on the constituents of such online identifier.

---

[367] See note 309 above.

[368] Section 9 of the DPA. See also Article 4(25) of the GDPR for a definition of 'Information society services'.

369 Data Protection Act 2018 Explanatory Notes 23 available at *http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf,* accessed on 15 November 2019.

370 The draft Code of Practice is available at *https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf,* accessed on 11 November 2019.

[371] Mc Cullagh et al 'National Adaptations of the GDPR' (note 364 above) 113.

5.3.2.3 Penalties for breaches

The DPA creates criminal offences for breaches which are similar to the old DPA. It builds on the old regime by introducing a new criminal offence to deal with emerging issues, such as re-identifying anonymised or pseudonymised personal data.[372] The rationale for creating this offence is informed by the UK's Digital Strategy.[373] The penalty for such an offence on conviction is a fine which is not limited to a maximum amount.[374] The DPA also extends liability to the directors of a corporate body or to partners in a partnership.[375] In this way, it has a wider scope than the GDPR. However, the downside is that the DPA does not impose imprisonment as a penalty for conviction of an offence.

5.4 NEW ZEALAND

5.4.1 An Overview of Statutory Data Protection in New Zealand

The NZ Bill of Rights[376] does not contain a freestanding right to privacy. However, it includes unlawful search and seizure protection for individuals.[377] The Privacy Act regulates the protection of data privacy in NZ in relation to the use, collection and disclosure of personal information held by private and public sector agencies. The objective of the Privacy Act is to afford protection to individual privacy in general accordance with the OECD Guidelines.[378] The Act only applies to the protection of living natural persons and excludes protection of juristic entities or deceased individuals.[379]

The Privacy Act contains 12 Information Privacy Principles (IPPs)[380] which create rights for individuals and obligations for agencies[381] to collect, access, store, retain, correct,

---

[372] Section 171 read with section 196(2) of the DPA.
[373] Data Protection Act 2018 Explanatory Notes (note 369 above) 18.
[374] Section 196(2) of the DPA.
[375] Section 198 of the DPA.
376 New Zealand Bill of Rights Act 1990 available at *http://www.legislation.govt.nz/act/public/1990/0109/latest/DLM224792.html*, accessed on 01 November 2019. The Preamble to the NZ Bill of Rights merely affirms the protection of human rights and commitment to the ICCPR.
[377] Ibid at section 21.
[378] Preamble of the Privacy Act.
[379] Section 2(1) of the Privacy Act.
[380] Part 2 of the Privacy Act.
[381] An 'agency' is defined in section 2(1)(a) of the Privacy Act as "any person or body of persons, whether corporate or unincorporated, and whether in the public sector or the private sector; and, for the avoidance of doubt, includes a department."

secure and disclose personal information. A breach of any of the IPPs or non-compliance with a code of practice by an agency amounts to interference with data privacy, which affords an individual the right to lodge a complaint with the Commissioner.[382] In terms of such complaints, Butler observes that the Privacy Act sets a high threshold because "mere misuse or dissemination of personal information is insufficient for a complaint to be upheld."[383] One advantage of the Privacy Act is that the Commissioner is required to carry out periodic review of the Act at intervals of not more than five years.[384]

The Privacy Act is enforced by the Commissioner that is granted the wide functions set out in section 13.[385] The Commissioner is described as a 'watchdog' for data privacy incursions arising from policy or legislation,[386] and plays an instrumental role in providing recommendations for data protection law reform, as discussed below.

5.4.2 Reform of the Statutory Data Protection Regime

In 2011, the NZ Law Commission completed a rigorous review of the Privacy Act, with the overall aim of modernising the Act.[387] Key considerations included consistency with international privacy instruments and the data privacy laws of NZ's trading partners as well as ensuring that the Privacy Act remains relevant and effective to withstand the challenges posed by technological developments.[388] The impact of technologies on data privacy were extensively discussed in Chapter 10 of the Stage 4 Report.[389] Six recommendations were made to reform the data protection regime to keep pace with technological developments.[390]

---

[382] Section 66 of the Privacy Act.

[383] P Butler 'The Case for a Right to Privacy in the New Zealand Bill of Rights Act' (2013) 11 *NZJPIL* 213.

[384] Section 26 of the Privacy Act.

[385] Specific functions in relation to monitoring technological developments are discussed in Chapter 4.

[386] Ibid at 221.

[387] The review commenced in 2006 and consisted of a four-stage process. Notably, Stage 1 focussed specifically on the privacy values, the impact of technology and international trends, whilst Stage 4, in particular, reviewed the Privacy Act and contained 136 key recommendations for reform.

[388] Law Commission's Review of the Privacy Act 1993: Stage 4 (Report 123) (note 252 above) at 1.15.

[389] Ibid at 249.

[390] Ibid at 22. The Law Commission's Review Report's recommendations in relation to technology can be summarised as follows: -

(1) "The word 'computer' be deleted from section 13(1)(n)";
(2) The IPPs should be retained but reviewed every five years to ensure that the Privacy Act responds effectively to data privacy issues raised by technological advancements;
(3) A Privacy by Design Expert Panel, to be formed by the Commissioner, should be considered to promote data privacy by design and create awareness of the use of privacy enhancing technologies;
(4) Adoption by NZ of a policy providing direction on compiling a privacy impact assessment;
(5) Guidance on privacy impact assessments in the public sector should be provided and published on the State Services Commission's website; and

Although the review extensively considered the challenges that technological developments pose to data protection, the Law Commission's recommendations did not require that enhanced protection provisions be included in the new legislation. For instance, in respect of the concept of privacy by design, the Law Commission recommended that the Privacy Commissioner should consider setting up a Privacy by Design Panel of experts to promote and further privacy by design and to create awareness of PETs.

The new Privacy Bill was introduced in Parliament on 20 March 2018. It incorporates the majority of the Law Commission's recommendations and also includes some of the recommendations arising from the review initiated by the Commissioner in 2016, that was conducted in accordance with section 26 of the Privacy Act.[391] To keep pace with the current digital climate, the Commissioner recommended that law reform encompass further changes, including amongst others, introducing a higher civil penalty ($1 million for organisations and $100,000 for individuals) who seriously breach their obligations to be imposed in cases of severe privacy breaches, protection of an individual against unexpected identification from data that has been anonymised and the introduction of the data portability right.[392]

In its submissions on the Privacy Bill once released for comment, the Commissioner highlighted that the Bill is not adequate in the light of the data-driven economy due to developments in data science and information technology. For NZ data protection law to be considered adequate, comprehensive and fit for purpose in the digital economy, the Commissioner proposed that additional reform be included in the Privacy Bill including the right to re-identification, the right to data portability, and the right to erasure, algorithmic transparency and automated decision-making.

The NZ Human Rights Commission ("HC") also made submissions on the Privacy Bill. Referring to the GDPR, it described the Privacy Bill as "antiquated and conservative in its

---

(6) The Commissioner should consider issuing a code of practice or guidance governing the use and processing of biometrics.

391 Privacy Commissioner's 'Briefing for the Incoming Minister of Justice: Hon Andrew Little Office of the Privacy Commissioner' dated October 2017 available at *https://privacy.org.nz/assets/Uploads/Briefing-for-Incoming-Minister-October-2017.pdf,* accessed on 01 November 2019.

[392] Ibid at 3-4.

approach to affirming and protecting privacy and human rights."[393] The HC criticised the Bill for not making reference to any freestanding right to privacy and called for consistency between the GDPR and the Privacy Bill, asserting that the GDPR addresses the emerging challenges to the right to privacy and is far more advanced than the Privacy Bill in responding to the current technological climate. The HC further proposed that the Privacy Bill should be substantially aligned to the data protection rights contained in the GDPR, including the right to erasure, the right to data portability, the concept of privacy by design and the rights in relation to automated decision making and profiling.

The Privacy Bill seeks to modernise the Privacy Act mainly by affording the Commissioner with more enforcement powers and by including more severe penalties for non-compliance.[394] Notably, it does not incorporate the additional law reform recommendations submitted by the Commissioner and the HC.

---

[393] New Zealand Human Rights Commission 'Submission on the Privacy Bill' 3 available at *https://www.hrc.co.nz/files/1115/4042/8222/Human_Rights_Commission_Submission_on_the_Privacy_Bill_-__24_May_2018.pdf*, *accessed* on 30 November 2019.

[394] The key changes to the NZ data privacy legal regime introduced by the Privacy Bill are summarised as follows:

(1) cloud service providers and information transmitted overseas for storage and processing on behalf of an agency fall within clause 8 of the Privacy Bill which holds an agency accountable for information held by another agency as its agent;

(2) agencies are required to issue mandatory data breach notifications by reporting data breaches to the Commissioner and the individual affected as soon as reasonably practicable[394] in instances where the breach has caused or there is a risk for causing harm clause[394] to the data subject. Failure to comply with the mandatory breach notification requirement is an offence for which a maximum fine of $10,000 can be levied against the infringing agency. In addition, the Commissioner can name and shame the infringing agency by publishing its identity if it is in the public interest to do so;

(3) compliance notices can be issued by the Commissioner to direct an agency to refrain or commit an act to demonstrate compliance with the Privacy Act. The process to issue the compliance notice is set out in the Privacy Bill.[394] The Human Rights Review Tribunal will then enforce the notice or consider an appeal by the agency served with the notice and can direct that the agency complies with the notice or take action to remedy the breach.[394] A fine of up to $10,000 can be levied against the agency for failure to comply with an order;

(4) the Commissioner's information-gathering powers are expanded by the Privacy Bill, empowering it to issue binding decisions on access to information requests by data subjects. The Commissioner is empowered to issue a directive to an agency to make the information requested available to the data subject within a timeframe up to the discretion of the Commissioner, which may be shorter than the default timeline of 20 working days.[394] The penalty for non-compliance with the Commissioner's directive on the information request will attract a maximum fine of $10,000; and

(5) two new criminal offences are introduced, namely, misleading an agency to obtain access to another person's personal information[394] and destruction of a document containing personal data, knowing that a request has been made for it.[394] Penalties for such offences would increase to $10,000 which is a

5.5 CONCLUDING REMARKS

Greenleaf asserts that "[D]ata protection laws outside Europe already converge on more than ½ of the higher standards that have been required in Europe since the 1990s." The GDPR is regarded as a 'gold standard' by certain countries to reform their data protection as it is recognised as international best practice, with 120 countries having enacted EU-style data privacy laws [395]

It is clear that the GDPR sets high standards to enhance data privacy protection reform in the ever-evolving digital world. Although the UK is exiting the EU, it cannot depart from the protection afforded by the GDPR and has taken legislative steps to ensure that its domestic data protection regime is aligned to the GDPR. To some extent, NZ has attempted to reform its data protection regime to take the GDPR into account; however technologically robust data protection requirements have been excluded in the Privacy Bill.

The POPIA should be amended to include a similar periodic review mechanism as provided for in the Privacy Act, which is critical to ensure that the POPIA remains adequate and effective in a rapidly evolving technological environment. The POPIA should be aligned to the GDPR to provide a 'like-for-like' level of protection for SA, especially because the GDPR has far-reaching consequences for South African businesses due to its extraterritorial application.

---

substantial increase on the current penalties imposed by the Privacy Act amounting to fines of up to $2,000.

[395] G. Greenleaf 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108' (2011) 2 *International Data Privacy Law* 77.

CHAPTER 6: OVERVIEW, CONCLUSION AND RECOMMENDATIONS

6.1 OVERVIEW

The 4IR has brought data privacy challenges into the limelight at both national and international levels. In light of these challenges, this research investigated the adequacy of the South African data protection regulatory regime to uphold data privacy with a particular focus on the Information Regulator's mandate to monitor technological developments to mitigate the adverse effects thereof on data privacy protection. Data privacy challenges caused by technological advancements are of international concern due to the borderless nature of the technologies used to collect, store or transmit personal data globally. The research thus took into account the technological foresight activities of well-established foreign DPAs and the reform of data protection legislation in the EU, the UK and NZ. In order for the POPIA to remain relevant, adequate and effective in the digital age, this Chapter sets out recommendations for consideration by the Information Regulator to enhance the protection of personal information in SA.

6.2 CONCLUSION

A key feature of this research was an analysis of the Information Regulator's mandate to monitor developments in technology to mitigate its adverse effects on the protection of personal information. Since the POPIA has not yet entered into force and effect, it was critical to examine the technological foresight work conducted by well-established foreign DPAs in the UK and NZ to determine if SA can learn any lessons from these jurisdictions. In executing its mandate, the core functions of the Information Regulator were examined in detail.

Turning to the technological foresight monitoring work of foreign DPAs, the NZ Commissioner and UK's ICO[396] take a proactive rather than a reactive stance when monitoring technological developments. The activities undertaken by these foreign DPAs can serve as sound guidelines for the Information Regulator to plan or structure its technological foresight activities. A lesson learnt from the UK and NZ DPAs is the need for the

[396] See discussion in Chapter 4, paragraphs 4.3 and 4.4.

Information Regulator to gather expertise in the ICT field to keep abreast of the impact of new technologies on data privacy.

It has been 15 years since the SALRC launched its investigation into the protection of data privacy and since then there has been a shift in the global digital landscape, with significant implications for data privacy protection. SA will therefore need to keep pace with developments in international best practices. Foreign jurisdictions, such as NZ, the EU and the UK, have embarked on reforming their data protection regulatory regimes to address technological impacts.

The analysis of the EU data protection regime demonstrated that the EU Directive was repealed in its entirety by the GDPR largely because it lacked substance to protect data privacy in the digital age. This research focussed on the novelty provisions of the GDPR encompassing enhanced rights for data subjects and the obligations imposed on data controllers to prevent data privacy infringement occasioned by the use of technology.[397] The POPIA does not specifically deal with these novelty provisions. Unlike SA, the EU also regulates online privacy through the ePrivacy Directive. Furthermore, the extra-territorial application of the GDPR has implications for South African businesses.[398] Scholars refer to the GDPR as a 'gold standard' for countries to reform their data protection as it is recognised as international best practice.

Since the POPIA was largely premised on the EU Directive, it is important that it be reformed in line with the provisions discussed in Chapter 5, paragraph 5.2 above. The additional reforms adopted by the UK and NZ that afford data subjects enhanced protection of personal information should also be taken into account. Although there is no one-size-fits approach to regulatory reform, taking into account that risks associated with technological advancements transcend territorial borders, data protection is no longer limited to domestic protection.

[397] See discussion in Chapter 5, paragraph 5.2.

6.3 RECOMMENDATIONS

6.3.1 Recommendations for Technological Foresight

Section 47(7) of the POPIA only requires the Information Regulator to appoint a person with specialist knowledge temporarily or to assist on a particular matter. It is submitted that successful technological foresight activities require that technical expertise form part of the Information Regulator's structure since data protection as a whole and ICT expertise, in particular, have been described as "moving targets" due to existing new technologies and the rapid rate at which emerging technologies are likely to increase. Alternatively, in the short term, the Information Regulator should adopt the ICO's "intelligence hub" model to gather information and intelligence from various sources, such as academics, journalists and technologists. In the long term the Information Regulator may elect to set up a panel of experts in line with its independence so that it can respond promptly to the dynamic privacy and technological environment.

Notwithstanding that the POPIA is a technologically neutral piece of legislation, it is recommended that, like the ICO, the Information Regulator should develop binding codes of conduct to regulate the use of certain technologies so that any breach thereof will trigger the penalty system to enforce the data subject's rights.[399]

As educator, in creating awareness of the lawful processing conditions of personal information through its Outreach and Research Committee, the Information Regulator should ensure that the Public Awareness Strategy specifically includes, as a standing item, the recent types of technological developments which impact data privacy rights so as to create awareness of the application of lawful processing conditions when using a particular technology.

To remain at the forefront of technological developments, it is also submitted that the Information Regulator should participate as an active member in international forums which deal with technology impacting data privacy matters.[400] The Regulator should also focus on a

---

[398] See discussion in Chapter 5, paragraph 5.2.2.2.

[399] See discussion in Chapter 4, paragraphs 4.2.1.

[400] Such as the International Working Group on Data Protection in Telecommunications, the Internet Privacy Engineering Network, and the OECD Working Party on Information Security and Privacy.

technology strategy as adopted by the DPAs in NZ and the UK by setting out specific technology goals to tackle new technologies or disruptive business models and address how these could be regulated in certain sectors.

6.3.2 Recommendations for Reform

The concept of privacy by design[401] is a valuable innovative obligation in the GDPR which is a preventative measure to enhance data privacy protection by ensuring that technologies used to process personal data are designed to incorporate controls to mitigate the risks of unlawful processing. Technology impedes free and informed consent and the use of technology such as Big Data allows personal data to be reused outside the purpose limitation for which consent was obtained. The function and significance of consent as a legal ground is therefore diluted.[402] The POPIA does not include the design and default obligation to ensure that privacy safeguards are 'built in' to the technology from the design stage. The Information Regulator's research strategy[403] will need to take into account preventative measures to mitigate the impact of technology by focusing on data protection by design and default requirements. To promote PETs, the POPIA will need to be amended to explicitly include privacy by design and default as a standard obligation, as is currently regulated by the GDPR.

In order to counter the negative effects of technology from the outset, it is recommended that provision be made design and default under the accountability condition of the POPIA. Alternatively, it is strongly recommended that the Information Regulator consider issuing a binding code of conduct that targets the manufacturers of technologies to ensure that privacy controls are embedded from the design stage (data protection by design and default) of the technologies.

Regulation of the online environment, particularly in relation to electronic communications services in public communication networks, requires a higher degree of data privacy protection. In the EU, the ePrivacy Directive, which will be replaced by the ePrivacy Regulation to complement the GDPR, requires EU member states to ensure that consent is obtained from a user before cookies can be stored or accessed from his or her smartphone, computer or any other device connected to the internet. The protection afforded by the ePrivacy Directive extends to tracking technology and direct marketing. The POPIA, in its

[401] See discussion in Chapter 5, paragraph 5.2.2.6.
[402] See discussion in Chapter 2, paragraph 2.2.4.4(b) (iii).

current form, does not deal with online privacy at all and there is no specific legislation in SA dealing with such. It is recommended that Information Regulator consider the requirements of the ePrivacy Directive and the proposed ePrivacy Regulation and recommend to Parliament the enactment of specific legislation or amendment of the POPIA to regulate online privacy in a holistic manner.

Given that the POPIA was premised on the provisions of the 1995 EU Directive, it would be remiss for the Information Regulator not to take into account the provisions of the GDPR when reforming data protection law in SA to counter the negative effects of rapid technological developments. It is strongly recommended that a holistic approach to data protection law reform in SA should be adopted and that the POPIA should be amended to include the following key GDPR provisions to afford a higher degree of protection of data privacy:

(a) The POPIA should incorporate the GDPR identifiability criterion, extending the POPIA application to all forms of data identifying a data subject, whether directly or indirectly and notwithstanding the technology used;[404]
(b) To afford like-for-like protection to data subjects and considering that some technologies process personal data outside of SA, the POPIA should also create an extraterritorial scope of application, subject to similar limitations imposed by the GDPR;
(c) To align the POPIA to the online reality, the definition of 'personal information' should be aligned to the GDPR definition of 'personal data' by extending the definition to include the 'online identifier' and 'location data';
(d) The term 'processing' in the POPIA should be expanded as defined in Article 4 of the GDPR so that operations on personal data, continued storage thereof and/or further processing by automated technologies such as Blockchain, cloud computing, Artificial Intelligence or machine learning fall squarely within the definition of processing and are therefore subject to the conditions for the lawful processing of personal information;
(e) The POPIA should include the GDPR requirements for consent and further include an obligation on the responsible party to prove that the data subject has consented to the processing of his or her personal information;[405]

---

[403] See discussion in Chapter 4, paragraph 4.2.
[404] See discussion in Chapter 5, paragraph 5.2.2.1.

(f) To enhance data protection rights and afford greater control of the movement or transmission of personal data, the POPIA should be amended to include the right to data portability subject to the conditions set out in Article 20(1) of the GDPR; and[406]

(g) The specific rights afforded in terms of the right to be forgotten provide internet users with better control of the use and accuracy of their personal data. Accordingly, it is submitted that section 24 of the POPIA should be more explicit to afford data subjects the right to request the erasure or further processing of their personal information held by responsible parties as provided for in Article 17 of the GDPR.

As noted in the NZ Privacy Bill, "since computers have become sufficiently ubiquitous as to need no reference and such reference" may have "the adverse effect of appearing to exclude other technologies", it is recommended that the word 'computer' should be removed from the Information Regulator's technology monitoring function to avoid excluding other technologies and to ensure that it is broad enough to cover all forms of technologies used to process personal information.

Finally, due to the technologically sensitive nature of data protection law, it is recommended that the POPIA should include a similar periodic review mechanism as provided for in the Privacy Act, which is an important provision to ensure that the POPIA remains adequate and effective in a rapidly evolving technological environment.

[405] See discussion in Chapter 5, paragraph 5.2.2.3.
[406] See discussion in Chapter 5, paragraph 5.2.2.5.

BIBLIOGRAPHY

1. **PRIMARY SOURCES**

1.1 South Africa

Statutes

Constitution of the Republic of South Africa Act No. 108 of 1996

Consumer Protection Act No. 68 of 2008

Electronic Communications and Transactions Act No. 25 of 2002

National Credit Act No. 34 of 2005

Protection of Personal Information Act No. 4 of 2013

Promotion of Access to Information Act No. 2 of 2000

Regulations relating to the Protection of Personal Information, 2017, published in accordance with Section 112(2) of the POPIA - GN R 2017 in *GG* 41105 (not yet proclaimed)

Case law

Bernstein v Bester NO 1996 (2) SA 751 (CC)

Black Sash Trust v Minister of Social Development and Others (Freedom Under Law NPC Intervening) (CCT48/17) [2017] ZACC 8; 2017 (5) BCLR 543 (CC); 2017 (3) SA 335 (CC)

H v W (2013) 2 All SA 218 (GSJ)

Investigating Directorate: Serious Economic Offences and others 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)

Jooste v National Media Ltd 1994 (2) SA 634 (C)

Ketler Investment CC Presentations v Internet Service Providers' Association 2014 (1) ALL SA 566 (GSJ)

NM and Others v Smith and Others (Freedom of Expression Institute as Amicus Curiae) 2007 (7) BCLR 751 (CC) 32

Minister of Justice and Constitutional Development and Others v Prince (Clarke and Others Intervening)

Mistry v Interim Medical and Dental Council of South Africa 1998 (4) SA 1127 (CC)

National Director of Public Prosecutions and Others v Acton (CCT108/17) [2018] ZACC 30; 2018 (10) BCLR 1220 (CC); 2018 (6) SA 393 (CC); 2019 (1) SACR 14 (CC)

O'Keeffe v Argus Printing and Publishing Co Ltd 1954 (3) SA 244(C)

Swanepoel v Minister van Veiligheid en Sekuriteit 1999 (4) SA 549 (T)

Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk 1977 (4) SA 376 (T)

1.3 International Law

Statutes and International Conventions

Data Protection Act of 2018 c 12

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

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

European Union (Withdrawal) Act 2018

New Zealand Bill of Rights Act 1990

Organisation for Economic Cooperation and Development (OECD), Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data, 23 September 1980,

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and

repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD)

The Privacy Act of 1993 No. 28

Privacy and Electronic Communications (EC Directive) Regulations, 2003

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 (General Data Protection Regulation)

Case law

Breyer v Bundesrepublik Deutschland Case C-582/14 ECLI:EU:C:2016:779

Google v. CNIL and *C-136/17, G.C. and Others v. CNIL* C-507/17

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

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

Peter Nowak [2017] Case C-434/16 EU:C:2017:994

Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV, Case C-673/17 ECLI:EU:C:2019:246

Salvatore Manni [2017] Case C-398/15 EU:C:2017:197

Weltimmo S.R.O. V. Nemzeti A Datvedelmi Es Informacioszabadsagh Atosag (Hungarian Dpa), C-230/14 1.10.15

2. SECONDARY SOURCES

Books

AB Makulilo *African Data Privacy Laws* in Law, Governance and Technology Series 1ed (2017)

D Van der Merwe et al *Information Communications Technology* Law 2ed (2016)

I Currie et al *The Bill of Rights Handbook* 6ed (2013)

JM Burchell *Principles of Delict* 1 ed (1993)

J Neethling et al *Neethling's Law of Personality* 2 ed (2005)

LA Bygrave *Data Privacy Law: An International Perspective* (2014)

William RM Long et al *The Privacy, Data Protection and Cybersecurity Law Review* 5ed (2018)

Y Burns and A Burger-Smidt *A Commentary on the Protection of Personal Information Act* (2018)

Chapters in Books

A Roos 'Data Privacy Law' in D Van der Merwe, A Roos, T Pistorius, S Eiselen and S Nel (eds) *Information and Communications Technology Law* 2ed 2016

D Flaherty 'Controlling Surveillance: Can Privacy Protection Be Made Effective?' (2018) in Agre, P. and Rotenberg, M. (eds.) *Technology and Privacy: The New Landscape.* Cambridge, MA: The MIT Press: 167-192

G Greenleaf (2013a) Chapter 10: 'Data protection in a globalised network' in Brown, 1 (ed) *Research handbook on governance of the Internet.* Northampton, MA: Edward Elgar: 221-259

L Mitrou 'The General Data Protection Regulation: A Law for the Digital Age?' in Tatiana-Eleni Synodinou et al (ed) *EU Internet Law*: Springer (2017) 39-40

Other

Department of Telecommunications and Postal Services Concept Document: Establishment of the Presidential Commission on the Fourth Industrial Revolution in GN 764 *GG* 42078 of 4 December 2018.

Discussion Papers

South African Law Reform Commission Discussion Paper 109 (Project 124) 'Privacy and Data protection' (2005)

The South African Law Reform Commission Project 124 **'**Privacy and Data Protection Report' (2009)

Journal articles

A Giurgiu and TA Larsen ‘Roles and Powers of National Data Protection Authorities: Moving from Directive 95/46/EC to the GDPR: Stronger and More ‘European’ DPAs as Guardians of Consistency?’ (2016) 2 *The European Data Protection Law Review*

A Giurgiu and G Lommel, ‘A new Approach to EU Data Protection – More Control over Personal Data and Increased Responsibility’ (2014) 1 *Critical Quarterly for Legislation and Law*

A Roos 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position’ (2007) 124(2) *SALJ* 401

A Roos ‘Personal data protection in New Zealand: lessons for South Africa?’ (2008) 4 *Potchefstroom Electronic Law Journal*

B Batchelor and T Wazvaremhaka ‘Balancing financial inclusion and data protection in South Africa: *Black Sash Trust v Minister of Social Development’* (2019) 136(1) *SALJ*

B Koops ‘The Trouble with European Union Data Protection law’ (2014) 4(4) *International Data Privacy Law*

CJ Hoofnagle et al ‘The European Union general data protection regulation: what it is and what it means?’ (2019) 28(1) *Information & Communications Technology Law*

C Raab and I Szekely ‘Data Protection Authorities and Information Technology’ (2017) *Computer law & Security Review* 421–33

DB-Wills ‘The technology foresight activities of European Union data protection authorities’ (2017) 116 *Technological Forecasting & Social Change* 142

G. Greenleaf ‘The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108’ (2011) 2 *International Data Privacy Law*

Hustnix ‘EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection’ in Cremona M et al (ed) *New Technologies and EU Law* 1ed Oxford (2017)

J Burchell ‘The Legal Protection of Privacy in South Africa: A Transplantable Hybrid’ (2009) 13.1 *EJCL*11

J Neethling ‘Features of the Protection of Personal Information Bill’ (2013) 75 Journal of Contemporary Roman-Dutch Law 241-255

J Van den Hoven et al ‘Privacy and Information Technology’ (2018) *The Stanford Encyclopedia of Philosophy*

LA Bygrave ‘Data Protection by Design and by Default: Deciphering the EU’s Legislative Requirements’ (2017) 4 *Oslo Law Review*

M Burri and R Shcar ‘The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy’ (2016) *Journal of Information Policy*

N Purtov ‘The law of everything. Broad concept of personal data and future of EU data protection law’ (2018) *Law, Innovation and Technology*

P Butler ‘The Case for a Right to Privacy in the New Zealand Bill of Rights Act’ (2013) 11 *NZJPIL*

R Luck ‘POPI - is South Africa keeping up with international trends?’ (2014) 44 *De Rebus* 84

S Bu-Pasha ‘Cross-border issues under EU data protection law with regards to personal data protection’ (2017) 26 (3) *Information & Communications Technology Law*

W Maxwell ‘Technology neutrality in Internet, telecoms and data protection regulation’ (2014) *Computer and Telecommunications L. Rev*

Dissertations

J Neethling *Die Reg op Privaatheid* (LLD thesis Unisa 1976)

Online Sources

Article 29 Data Protection Working Party ‘Guidelines on the right to data portability’ 6/EN WP 242 rev.01 adopted on 13 December 2016 available at *https://iapp.org/media/pdf/resource_center/WP29-2017-04-data-portability-guidance.pdf*, accessed on 12 September 2019

Article 29 Data Protection Working Party “Guidelines on consent under Regulation 2016/679” WP259rev.01, 10 April 2018 18 available at *https://webcache.googleusercontent.com/search?q=cache:l-b4dUk35iAJ:https://ec.europa.eu/newsroom/article29/document.cfm%3Faction%3Ddisplay%26doc_id%3D51030+&cd=1&hl=en&ct=clnk&gl=za*

Article 29 Data Protection Working Party, Opinion 04/2007 on the Concept of Personal Data (WP 136) 01248/07/EN, available at *https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf*, accessed on 01 November 2019

CJ Bennett ‘The Data Protection Authority: Regulator, Ombudsman, Regulator or Campaigner?” Presentation at 24th International Conference of Data Protection and Privacy Commissioners’ 9-11 September 2002, available at *web.uvic.ca:8080/polisci/bennett/pdf/Cardiff.pdf* , accessed on 11 November 2019

Data Protection Act 2018 Explanatory Notes 23 available at *http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf*, accessed on 15 November 2019.

D Milo and G Palmer ‘South Africa- New comprehensive data privacy law passed’ *Linklaters* 31

January 2014, available at *http://www.linklaters.com/Insights/Publication1403Newsletter/TMT-News-31-January-2014/Pages/SouthAfrica-New-comprehensive-data-privacy-lawpassed.aspx,* accessed on 20 June 2019

European Data Protection Supervisor 'Technology Monitoring' available at *https://edps.europa.eu/data-protection/our-work/technology-monitoring_en*, *accessed* on 13 April 2019

European Union's Article 29 Data Protection Working Party 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' WP 223 (2014) available at *https://www.dataprotection.ro/servlet/ViewDocument?id=1088*, accessed on 20 July 2019

Gartner Glossary available at https://www.gartner.com/en/information-technology/glossary/cloud-computing, accessed on 11 July 2019

GDPR website available at *https://gdpr.eu/eu-gdpr-personal-data/,* accessed on 07 December 2019

Global Convergence of Data Privacy Standards and Laws: 'Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi' available at *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3184548,* accessed on 10 April 2019

ICO's "Guidance on the use of cookies and similar technologies" dated 03 July 2019, pages 6-7, available at *https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/*, *accessed* on 03 October 2019

ICO website for an overview of the PECR available at *https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/*, accessed on 02 October 2019

ICO's "Guide to Privacy and Electronic Communications Regulations" available at *https://ico.org.uk/for-organisations/guide-to-pecr/*, accessed on 02 October 2019

ICO website "The Guide to the Sandbox (beta phase)" available at *https://ico.org.uk/for-organisations/the-guide-to-the-sandbox-beta-phase/*, accessed on 05 October 2019

ICO website "Tech and Innovation" available at *https://ico.org.uk/about-the-ico/what-we-do/tech-and-innovation/*, accessed on 05 October 2019

ICO's 'Opinion on the use of live facial recognition technology by law enforcement in public places' 31 October 2019 available at *https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf*, accessed on 25 November 2019

ICO 'CCTV Codes of Practice' available at *https://ico.org.uk/media/1542/cctv-code-of-practice.pdf*, *accessed* on 25 November 2019

ICO 'Data Sharing Code' available at *https://ico.org.uk/media/2615361/data-sharing-code-for-public-consultation.pdf*, accessed on 02 November 2019

ICO 'Data protection by design and default' available at *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/*, accessed on 10 November 2019

Information Regulator Terms of Reference "Outreach and Research Committee" available at *http://www.justice.gov.za/inforeg/docs/InfoRegSA-TOR-ORcommittee.pdf*, accessed on 20 September 2019

Information Regulator presentation on "Briefing of the Portfolio Committee on Justice and Correctional Services" dated 24 April 2018 available at *https://www.ellipsis.co.za/wp-content/uploads/2018/05/Information_Regulator_Briefing_24-April_2018.pdf*, accessed on 30 September 2019

Information Regulator presentation on "Briefing of the Portfolio Committee on Justice and Correctional Services" dated 24 April 2018 available at *https://www.ellipsis.co.za/wp-content/uploads/2018/05/Information_Regulator_Briefing_24-April_2018.pdf* accessed on 30 September 2019

Information Commissioner's Office 'Technology Strategy 2018-2021' available at *https://ico.org.uk/media/about-the-ico/documents/2258299/ico-technology-strategy-2018-2021.pdf*, accessed on 02 October 2019

Information Commissioner's Office "Innovation Plan" dated April 2017 available at *http://www.gov.uk/government/publications/ico-innovation-plan*, accessed on 02 October See ICO website "Guidance Index" available at *https://ico.org.uk/for-organisations/guidance-index/data-protection-act-1998/*, accessed on 02 October 2019

ISACA 'Enforcing Data Privacy in the Digital World' available *http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Enforcing-Data-Privacy-in-the-New-Digital-World.aspx*, accessed on 13 April 2019

Law Commission's Review of the Privacy Act 1993: Stage 4 (Report 123) dated June 2011 available at *https://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R123.pdf*, accessed on 02 October 2019

L. Mitrou "Data Protection, Artificial Intelligence and Cognitive Services: Is The General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof?" December 2013 available at *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914* accessed on 31 July 2019

Media release: Meeting Technology Challenges Head On: Modern Tools for Modern Problems dated 2 August 2011 available at *https://www.privacy.org.nz/news-and-publications/statements-media-releases/media-release-meeting-technology-challenges-head-on-modern-tools-for-modern-problems/*, *accessed* on 02 October 2019

Media publication of the Department for Digital, Culture, Media & Sport *and* Home Office available at *https://www.gov.uk/government/collections/data-protection-act-2018*, accessed on 02 October 2019

Mc Cullagh et al 'National Adaptations of the GDPR' (2019) *Collection Open Access Book* available at *https://wp.me/p6OBGR-3dP*, accessed on 04 November 2019

M Hildebrandt and L Tielemans 'Data Protection by Design and Technology Neutral Law' (2013) *Computer Law & Security Review* 509-52 available at *http://www.sciencedirect.com/science/article/pii/S0267364913001313*, accessed on 2 September 2019.

M Kuneva, 'Keynote Speech SPEECH/09/156' (Roundtable on Online Data Collection, Targeting and Profiling' available *at http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm*, accessed on 30 March 2019

New Zealand Department of Internal Affairs website available at *https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/*, accessed on 02 October 2019

New Zealand Human Rights Commission 'Submission on the Privacy Bill' available at *https://www.hrc.co.nz/files/1115/4042/8222/Human_Rights_Commission_Submission_on_the_Privacy_Bill_-__24_May_2018.pdf*, *accessed* on 30 November 2019

Office of the Privacy Commissioner's website available at *https://www.privacy.org.nz/the-privacy-act-and-codes/privacy-act-and-codes-introduction/*, accessed on 01 October 2019

Organisation for Economic Co-operation and Development 'The Evolving Privacy Landscape: 30 Years After the OECD Guidelines' 06 April 2011 at 4-6 available at *https://www.oecd-ilibrary.org/the-evolving-privacy-landscape-30-years-after-the-oecd-privacy guidelines_5kgf09z90c31.pdf?itemId=%2Fcontent%2Fpaper%2F5kgf09z90c31-en&mimeType=pdf*,accessed on 25 November 2019.

Office of the Privacy Commissioner's Technology Strategy entitled 'Making the Future Working with business to create a smarter, brighter future for privacy' dated December 2014 available at *https://www.privacy.org.nz/assets/Files/Policies-and-values-transparency/Making-the-Future-Working-with-business-to-create-a-smarter-brighter-future-for-privacy.pdf*, *accessed* on 02 October 2019

Office of the Privacy Commissioner's Statement of Intention 2017-2021 available at *https://www.privacy.org.nz/assets/Uploads/OPC-Statement-of-Intent-2017-2022.pdf*, accessed on 02 October 2019

Proposal for a Regulation of the European Parliament And Of The Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

COM/2017/010 final - 2017/03 (COD) available at *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010*, accessed on 2 December 2019

Privacy Commissioner website link to guidance Notes published available at *https://privacy.org.nz/news-and-publications/guidance-resources/*, accessed on 03 October 2019

Privacy Commissioner's website available at *https://privacy.org.nz/search/SearchForm?Search=big+data&Sections%5B1313%5D=1313&searchlocale=en_NZ&action_results=Go*, accessed on 03 October 2019

Privacy Commissioner's 'Public Statement about bulk disclosure of smart meter data', available at *https://www.privacy.org.nz/assets/Uploads/Open-letter-to-retailers-and-distributors-re-smart-meters-A504260.pdf*, accessed on 25 November 2019

Privacy Commissioner's 'Briefing for the Incoming Minister of Justice: Hon Andrew Little Office of the Privacy Commissioner' dated October 2017 available at *https://privacy.org.nz/assets/Uploads/Briefing-for-Incoming-Minister-October-2017.pdf*, accessed on 01 November 2019

Reed Smith 'One year of GDPR – lessons learned by the ICO' 4 June 2019, available at *https://www.technologylawdispatch.com/2019/06/privacy-data-protection/one-year-of-gdpr-lessons-learned-by-the-ico/*, accessed on 27 November 2019

Ryngaert, C & Taylor, M 'Symposium on the GDPR and International Law: The GDPR as Global Data Protection Regulation?' (2020) available at *https://www.cambridge.org/core/services/aop-cambridge-core/content/view/CB416FF11457C21B02C0D1DA7BE8E688/S2398772319000801a.pdf/gdpr_as_global_data_protection_regulation.pdf accessed on 02 January 2020,* accessed on 09 November 2019

Speech Delivered by Communications Deputy Minister Pinky Kekana at the Microsoft Annual Digital Summit in Sun City on 23 May 2019 available at *https://www.doc.gov.za/speech-delivered-communications-deputy-minister-pinky-kekana-microsoft-annual-digital-summit-sun*,accessed on 30 September 2019

Submission by the Office of the Privacy Commissioner on the Law Commission's Review of the Privacy Act 1993: Stage 4 dated 14 June 2010 at 82 available *https://privacy.org.nz/the-privacy-act-and-codes/privacy-law-reform/new-zealand-law-commission-privacy-review/*, accessed on 01 October 2019

T Mulder 'Health Apps, their Privacy Policies and the GDPR' (2019) 10 (1) *European Journal of Law and Technology* 7 available at *http://ejlt.org/article/view/667/897*, accessed on 09 November 2019

Telecommunications Information Privacy Code 2003 available at *https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/telecommunications-information-privacy-code/*, *accessed* on 09 October 2019

The European Parliament's Study on the 'Blockchain and the General Data Protection Regulation" Can distributed ledgers be squared with European data protection law?' available at

https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf, accessed on 10 October 2019

The Terms of Reference of the Enforcement Committee was signed on 18 April 2019 available at https://www.justice.gov.za/inforeg/docs/InfoRegSA-TOR-EFcommittee.pdf, accessed on 12 August 2019

The revised Withdrawal Agreement and Political declaration is available at *https://www.gov.uk/government/publications/new-withdrawal-agreement-and-political-declaration accessed*, on 15 November 2019

United Nations Conference on Trade and Development 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' available at *https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_summary_en.pdf*, accessed on 10 April 2019

World Economic Forum 'Data Policy in the Fourth Industrial Revolution: Insights on personal data' available at *https://www.weforum.org/whitepapers/data-policy-in-the-fourth-industrial-revolution-insights-on-personal-data*, accessed on 01 April 2019

World Economic Forum 'What is the Fourth Industrial Revolution?' available at *https://www.weforum.org/agenda/2016/01/what-is-the-fourth-industrial-revolution/*, accessed on 10 April 2019

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

13 August 2019

Ms Sarika Ramcharan (200104529)
School of Law
Howard College Campus

Dear Ms Ramcharan,

Protocol reference number: HSS/0539/019M
Project title: How will the Information Regulator manage and control advancements in technology to minimise its adverse effects on the protection of personal information

Full Approval – No Risk / Exempt Application

In response to your application received 06 June 2019, the Humanities & Social Sciences Research Ethics Committee has considered the abovementioned application and the protocol has been granted **FULL APPROVAL.**

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment /modification prior to its implementation. In case you have further queries, please quote the above reference number.

PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

The ethical clearance certificate is only valid for a period of 3 years from the date of issue. Thereafter Recertification must be applied for on an annual basis.

I take this opportunity of wishing you everything of the best with your study.

Yours faithfully

.....
Professor Urmilla Bob
University Dean of Research

/ms

Cc Supervisor: Mr Lee Swales
cc. Academic Leader Research: Dr Donrich Thaldar
cc. School Administrator: Mr Pradeep Ramsewak

Humanities & Social Sciences Research Ethics Committee
Dr Rosemary Sibanda (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 **Facsimile:** +27 (0) 31 260 4609 **Email:** [redacted] / [redacted] / [redacted]
Website: [redacted]