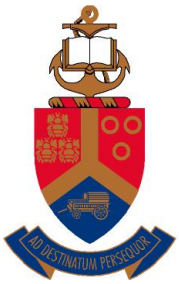


UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

The Regulation and Enforcement of Consumer Privacy in the Digital Age in South Africa

by

Salim Musa Lvuyo Salim
18336452

Mini-dissertation submitted in partial fulfilment of the requirements for the degree

Master of Laws in Mercantile Law

In the

Faculty of Law

University of Pretoria

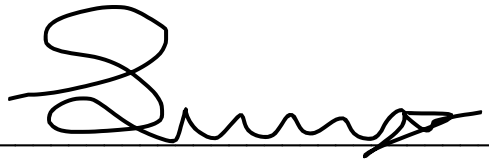
April 2025

Supervisor: Dr PT Magau

TABLE OF CONTENTS

Declaration

1. I understand what plagiarism is and am aware of the University's policy in this regard.
2. I declare that this mini-dissertation is my own original work. Where other people's work has been used (either from a printed source, internet or any other source), this has been properly acknowledged and referenced in accordance with the requirements as stated in the University's plagiarism prevention policy.
3. I have not used another student's past written work to hand in as my own.
4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

Signature 

Acknowledgements

I would like to thank the dedicated staff at Nando's Atterbury for keeping me nourished with excellent food during the many all-nighters spent completing this mini-dissertation.

I would also like to thank Dr Magau for his patience, dedication, and guidance throughout the supervision of this mini-dissertation.

Summary

This study examines the strengths and weaknesses of South Africa's legal framework for consumer privacy rights, focusing on key provisions from the *Constitution of the Republic of South Africa*, 1996, *the Electronic Communications and Transactions Act* 25 of 2002, the *Consumer Protection Act* 68 of 2005, and the *Protection of Personal Information Act* 4 of 2013. The study identifies weaknesses in South Africa's current consumer privacy framework such as the low administrative fine amount imposed for privacy violations, the lack of Artificial Intelligence (AI) specific legislation and the absence of an explicit notification period to consumers in instances of a data breach. Moreover, the absence of a requirement for certain suppliers to have Information Officers located in South Africa, and the inability of the Information Regulator to award damages directly to consumers are also some of the challenges discussed in the study. To remedy these weaknesses, the study delves into a comparative analysis to draw lessons from the European Union and India's consumer privacy framework for possible application in enhancing South Africa's consumer privacy framework. The study concludes that while South Africa has made some progress in revamping its privacy framework in the past years, further amendments are necessary to align South Africa with global standards to effectively safeguard consumer privacy rights in the digital age.

CHAPTER ONE

RESEARCH OUTLINE AND CONTEXT

1.1 Introduction

In the digital age, the widespread collection and use[1] of consumers'[2] personal information[3] has become foundational to the operation of many online platforms, creating a need for modern legislative privacy protections.[4] Before the promulgation of the various pieces of legislation that specifically provide for the regulation and enforcement of consumer privacy in South Africa, consumer privacy was primarily governed by the common law until 1993 when the *Interim Constitution* was adopted.[5] South African privacy law was and is governed by the *Constitution*,[6] common law,[7] the *Consumer Protection Act*,[8] the *Electronic Communications and Transactions Act,*[9] and eventually the *Protection of Personal Information Act*.[10]

---

1 Bottis and Bouchagiar 2018 *Open Journal Philosophy* 206; Rose 2021 *Brooklyn Journal of Corporate, Financial, and Corporate Law* 526.

2 Section 1 of the *Consumer Protection Act* 68 of 2008 *(CPA*); section 1 of the *Protection of Personal Information Act* 4 of 2013 (*POPIA*); The *CPA* defines a consumer as any person to whom goods or services are marketed, who uses or benefits from those goods or services-regardless of whether they were party to the transaction, or who enters into a transaction with a supplier. The *POPIA* defines a data subject as the person to whom personal information relates. While the definitions of 'data subject' in the *POPIA* and 'consumer' in the *CPA* are not identical, they overlap significantly in the context of online privacy involving personal information. Accordingly, the terms are used interchangeably in this mini-dissertation, with attention to context where necessary.

3 Section 1 of the *POPIA*; Swales 2021 *South African Journal of Science* 1; The *POPIA* defines personal information as any sort of identifiable information relating to a specific person.

4 Pelteret and Ophoff 2016 *Informing Science: The International Journal of an Emerging Transdiscipline* 277 and 278; Oyewole et al 2024 *Computer Science and IT Research Journal* 629, 630, and 632.

5 Section 13 *Interim Constitution of South Africa Act* 200 of 1993; Mtuze and Papadopoulos *"*Privacy and Data Protection" 312 and 313; *Bernstein and Others v Bester NO and Others* (CCT23/95) [1996] ZACC 2 paras 12,68, and 69 (*Bernstein* case); McQuoid-Mason *CILSA* 1982 135.

6 See section 14 of the *Constitution of the Republic of South Africa*, 1996 (*Constitution*); Currie and de Waal *Bill of Rights Handbook* 294,295, and 309.

7 Mtuze and Papadopoulos "Privacy and Data Protection" 312 and 313; *Jansen van Vuuren and Another NNO v Kruger* [1993] 2 All SA 619 (A) para 8 (*Jansen* case); *Bernstein* case paras 68 and 69; McQuoid-Mason 1982 *CILSA* 135.

8 Section 11 of the *Consumer Protection Act* 68 of 2008 (*CPA);* Nagel et al *Commercial Law* 762.

9 Section 43(1)(p) of the *Electronic Communications and Transaction Act* 25 of 2002 (*ECTA).*

10 See Preamble to the *POPIA;* Netshakhuma 2019 *Global Knowledge, Memory and Communication* 58; Mtuze and Papadopoulos "Privacy and Data Protection" 348.

Common law delictual principles were foundational in the early development of consumer privacy rights.[11] In the *Jansen* case,[12] the court dealt with the right to privacy and enforced privacy protections through the common law.[13] In this case, the first defendant disclosed the plaintiff's HIV status to third parties.[14] The plaintiff sought redress for damages via the *actio iniuriarum*.[15] This case serves as an illustration of underdeveloped and disjointed enforcement mechanisms available to consumers at the time who have had their privacy violated as they would have to navigate through the common law and potentially incur expensive litigation fees.[16] Due to the deficiencies mentioned above in enforcing consumer privacy rights through the common law, the need for specific legislative privacy provisions became evident.

The *Constitution* is South Africa's first statutory framework that enshrines the right to privacy.[17] The *Constitution* states that everyone has the right to privacy which includes the right to not have their home, person, possessions or communications searched or seized.[18] Section 38 of the *Constitution* allows an aggrieved person to approach a competent court for the enforcement of privacy rights.[19] Due to the *Constitution* being the supreme law of South Africa, consumer privacy rights are protected by way of ensuring that any act that violates consumer privacy is constitutionally invalid.[20] The *Constitution's* regulatory provisions addressing the consumer's right to privacy are not exhaustive.[21]

The *ECTA* and the *CPA* provide more specific criteria on what the right to privacy entails for consumers.[22] The *ECTA* provides for the disclosure of privacy policies to

---

11 Mtuze and Papadopoulos “Privacy and Data Protection” 312 and 313; *Bernstein* case paras 68 and 69; McQuoid-Mason 1982 *CILSA* 135.

12 *Jansen van Vuuren and Another NNO v Kruger* [1993] 2 All SA 619 (A) (*Jansen*).

13 *Jansen* case paras 9,10,14, and 43.

14 *Jansen* case paras 1-9.

15 *Jansen* case paras 8 and 9.

16 Swales 2022 *PER/PELJ* 3; Woker 2019 *Stell LR* 104.

17 Sections 1(a),7(1), and 14 of the *Constitution; Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* (CCT1/00) [2000] ZACC 12 para 9.

18 Section 14 of the *Constitution;* Currie and de Waal *Bill of Rights Handbook* 294,295, and 309.

19 Section 38 of the *Constitution*; Currie and de Waal *Bill of Rights Handbook* 73-75; Jephson *Constitutional Court Review* 2014 286; *Mukaddam v Pioneer Foods (Pty) Ltd and Others* (CCT 131/12) [2013] ZACC 23 para 40.

20 Section 2 of the *Constitution*; Currie and de Waal *Bill of Rights Handbook* 5.

21 Section 14 of the *Constitution*; Mtuze and Papadopoulos “Privacy and Data Protection” 309.

22 Section 43(1)(p) of the *ECTA*; sections 11 and 12 of the *CPA*; *Kelter Presentations v Internet Service Providers'* [2014] JOL 31136 (GSJ) paras 7 and 79 (*Kelter* case).

consumers concerning consumer's personal information.[23] Additionally, the *CPA* protects consumer privacy by providing consumers with the opportunity to control their receipt of direct marketing material.[24] Consumers who have experienced a privacy violation can seek redress through the designated out-of-court institutions which are consumer ombuds, consumer courts, National Consumer Commission, and the National Consumer Tribunal mechanisms provided for in the *CPA*.[25] These bodies can provide quick, affordable, efficient and accessible redress to consumers.[26] Although the *ECTA* and the *CPA* consist of provisions that provide for the protection and enforcement of consumer's privacy rights,[27] they are not specialised pieces of legislation that are primarily focused on the protection of consumers' privacy rights in the digital age.[28]

The *POPIA* is South Africa's first piece of privacy legislation which aims to give effect to the consumer's constitutional right to privacy,[29] in the digital age, by establishing mechanisms and standards that must be adhered to when processing[30] personal information.[31] The *POPIA* provides for processing principles that must be adhered to when processing consumer's personal information, these are, accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, data subject participation and security safeguards.[32] Privacy-related complaints can be brought to the Information Regulator,[33] who is tasked with enforcing and ensuring compliance with the *POPIA.*[34]

This study aims to identify weaknesses present in South Africa's consumer privacy framework. These identified weaknesses in South Africa's overall privacy framework

---

23 Section 43(1)(p) of the *ECTA*.
24 Sections 11 and 12 of the *CPA; Kelter* case para 79,
25 Sections 3(1)(h) and 69 of the *CPA;* Mupangavanhu 2012 *PER/PELJ* 322-331.
26 Woker 2019 *Stell LR* 113; Woker 2010 *Obiter* 230; van Heerden & Barnard 2011 *Journal of International Commercial Law* 136.
27 Section 43(1)(p) of the *ECTA*; sections 11 and 12 of the *CPA.*
28 Preamble and section 2(a)of the *POPIA;* Fritz 2021 *Constitutional Court Review* 1,2, and 5; van Eeden and Barnard *Consumer Protection Law in South* 567,568.
29 Section 14 of the *Constitution*; Currie and de Waal *Bill of Rights Handbook* 6th edition 294 and 295, and 309.
30 Section 1 of the *POPIA*; Processing in this *Act* means the collection, storage and distribution of personal information.
31 Preamble and section 2(a) of the *POPIA;* Fritz *Constitutional Court Review* 2021 1,2, and 5*;* Mtuze and Papadopoulos "Privacy and Data Protection" 348.
32 Section 4(1) of the *POPIA;* Adams et al 2021 *South African Journal of Science* 1 and 2.
33 Section 74 of the *POPIA;* Mtuze and Papadopoulos "Privacy and Data Protection" 370.
34 Section 40(1) of the *POPIA;* Mtuze and Papadopoulos "Privacy and Data Protection" 367.

include inadequate provisions for protections against Artificial Intelligence (AI)[35] and the Information Regulator being unable to award damages to consumers who have experienced a privacy breach.[36] Other identified weaknesses include the Information Regulator's administrative fine amount being too low[37] and the fact that the *POPIA* does not explicitly specify a time period in which a consumer must be informed about an alleged privacy breach.[38] The author argues that these identified weaknesses hamper the effectiveness of South Africa's consumer privacy framework. To remedy these identified weaknesses the author will provide an analysis of relevant legislative provisions contained in the European Union and India's consumer privacy framework. These relevant legislative provisions will then form part of the basis of the recommendations that could remedy the identified weaknesses in South Africa's consumer privacy framework.

1.2 Statement of the Problem

In contemporary times and the digital age, consumer privacy and protection of personal information have become more important than ever. Notwithstanding this, consumers remain exposed and vulnerable to issues affecting their personal information. The recent Pam Golding data breach, where clients' personal information was compromised,[39] illustrates the ongoing necessity and significance of robust privacy regulations and effective enforcement. Due to the rapidly changing digital consumer landscape,[40] robust privacy regulations and effectively enforced privacy provisions are needed to give full effect to the consumer's privacy rights in the digital age.[41] One reason for South Africa's comparatively underdeveloped privacy

---

35 "AI National Government Summit Discussion Document: South Africa's Artificial intelligence (AI) Planning: Adoption of AI by Government 16" available at https://www.dcdt.gov.za/images/phocadownload/AI_Government_Summit/National_AI_Government_Summit_Discussion_Document.pdf; Gravett 2020 *South African Public Law* 19-23.

36 Section 99(1) of the *POPIA*; Mtuze and Papadopoulos "Privacy and Data Protection" 372.

37 Section 109(1)(c) of the *POPIA.*

38 Section 22(2) of the *POPIA*; Roos 2023 *THRHR* 20.

39 BusinessTech "South African Property Giant Hit by Major Data Breach" available at https://businesstech.co.za/news/property/816277/warning-over-property-data-breach-in-south-africa/; ITWeb "Cyber Attack Rattles Real Estate Firm Pam Golding" available at https://www.itweb.co.za/article/cyber-attack-rattles-real-estate-firm-pam-golding/lLn14MmQoLwMJ6Aa.

40 Jones 2021 *Penn State* Journal *of Law and International Affairs* 220 and 221; Kozyreva et al 2020 *Psychological Science in the Public Interest* 105 and108.

41 Jones 2021 *Penn State* Journal *of Law and International Affairs* 228 and 235; Mtuze and Papadopoulos "Privacy and Data Protection" 313 and 314; Kurz et al 2014 *Journal of Experimental Social Psychology* 176.

framework[42] is its relatively slow implementation of dedicated privacy legislation, namely the *POPIA*.

The researcher submits that there are six identified weaknesses in South Africa's consumer privacy framework that hinder the effective enforcement and regulation of consumers' privacy rights in the digital age. There is currently no AI-specific legislation dealing with the privacy threats that AI may pose to consumers.[43] The lack of specific AI legislation on consumer privacy is a serious challenge and a weakness in South Africa's privacy framework because the unique set of threats that AI could pose to the right to privacy requires specific legislative intervention to protect the consumers' right to privacy.[44] For instance, some of the AI-related threats to consumer privacy include the surveillance capabilities of AI,[45] and AI's ability to degrade the control aspect of the right to privacy.[46] Another challenge in the current legal framework for consumer privacy is the fact that the *POPIA* does not permit the Information Regulator to award damages to consumers who have experienced patrimonial and non-patrimonial damages.[47] This is a weakness in the *POPIA* because court litigation entails high costs and is a potentially lengthy process,[48] especially for vulnerable consumers in South Africa.[49] Currently, the *POPIA* only allows for administrative fines of up to R10 million

---

42 See the relatively recent promulgation of the *POPIA; De Jager v Netcare Limited and Others* (42041/16) [2025] ZAGPPHC 141 para 2; *Bernstein* case para 65.

43 "AI National Government Summit Discussion Document: South Africa's Artificial Intelligence (AI) Planning: Adoption of AI by Government 16" available at https://www.dcdt.gov.za/images/phocadownload/AI_Government_Summit/National_AI_Government_Summit_Discussion_Document.pdf; Gravett 2020 *South African Public Law* 19-23; van der Merwe 2023 *Obiter* 942.

44 "AI National Government Summit Discussion Document: South Africa's Artificial Intelligence (AI) Planning: Adoption of AI by Government 16" available at https://www.dcdt.gov.za/images/phocadownload/AI_Government_Summit/National_AI_Government_Summit_Discussion_Document.pdf; van der Merwe 2023 *Obiter* 942; Gravett 2020 *South African Public Law* 2, and 5-7.

45 Elliot and Soifer 2022 *Frontiers in Artificial Intelligence* 4; Saheb 2023 *AI and Ethics* 369 and 374.

46 Section 23-25 of the *POPIA*; *National Media Ltd v Jooste 1996 (3) SA 262 (SCA)* paras 11 and 13-18; Eliot and Soifer 2022 *Frontiers in Artificial Intelligence* 1; Bartneck *An Introduction to Ethics in Robotics and AI* 2 and 24.

47 Sections 95(1), 99(1), and 109(1)(2) of the *POPIA;* Mtuze and Papadopoulos "Privacy and Data Protection" 372; van Eeden and Barnard *Consumer Protection Law in South Africa Act* 571.

48 Barnard 2021 *International Journal on Consumer Law and Practice* 45; *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* [2021] ZACC 3 para 49 (*AmaBhungane* case); Peté et a *Civil Procedure: A Practical Guide* 301.

49 *Nkuzi Development Association v Government of the Republic of South Africa and Another* [2001] 4 All SA 460 (LCC) para 4**;** *Magidiwana and other injured and arrested persons v President of the Republic of South Africa and others (No 2)* [2013] ZAGPPHC 292 (GNP) para 25.

for suppliers who violate its provisions.[50] This amount is too low and could be seen as a weakness because it is not sufficient to deter companies with annual turnovers in the billions of rands from committing privacy violations.[51] Additionally, the *POPIA* does not prescribe a specific time in which consumers are to be notified that their privacy may have been infringed.[52] This is a weakness because a consumer may not be able to timeously make necessary adjustments to lessen the impact of a data breach due to the data controller not having to provide notification to the consumer in a specified amount of time.[53] The *POPIA* does not require suppliers processing large amounts of consumers' special personal information[54] to have Information Officers[55] based in South Africa.[56] This is a weakness due to the high costs of serving legal documents to individuals or entities abroad and the administrative challenges of investigating and enforcing compliance against entities located outside the country's borders.[57] There is currently no statutorily mandated optout/opt-in registry in South Africa.[58] This is a weakness because it results in the privacy rights enshrined in the *CPA*[59] not being fully realised.

The above weaknesses in South Africa's current privacy framework hinder the effective regulation and enforcement of the consumer's right to privacy in South Africa. As the digital landscape continues to change,[60] so too must the legal mechanisms that

---

50 Section 109(1)(c) of the *POPIA;* Lockaht 2021 *South African Journal of Anesthesia and Analgesia* 571; van Eeden and Barnard *Consumer Protection Law in South Africa Act* 572.

51 Liu 2024 *Journal of Education, Humanities and Social Sciences* 2024 101; Kraus et al 2021 *IJEBR* 60.

52 Section 22(1)(b)(2) of the *POPIA;* van Eeden and Barnard *Consumer Protection Law in South Africa* 576-578.

53 Section 22(1)(b)(2) of the *POPIA;* van Eeden and Barnard *Consumer Protection Law in South Africa* 576-578.

54 Section 26 of the *POPIA*; Special personal information includes information about a consumer that relates to their race, sex life, biometric information, religious beliefs, religious beliefs, criminal behaviour, and trade union membership.

55 Section 55 of the *POPIA*; van Eeden and Barnard *Consumer Protection Law in South Africa* 578; An Information Officer is a designated individual within an entity that is tasked with ensuring compliance with the *POPIA.* An Information Officer is presumed to be easily accessible or the first touch point of the Information Regulator due to the Information Officer having to register as an Information Officer at the Information Regulator.

56 Sections 26-33 of the *POPIA*; Adams et al 2021 *South African Journal of Science* 2.

57 Peté et al *Civil Procedure: A Practical Guide* 142 and 143; Mtuze "Electronic Contracts (E-contracts) and E-commerce" *Africa* 63 and 64.

58 Schedule 3 in GN R2798 in GG 51436 of 28 October 2024.

59 Section 11 of the *CPA*; van Eeden and Barnard *Consumer Protection Law in South Africa* 559.

60 Jones 2021 *Penn State* Journal *of Law and International Affairs* 220 and 221; Kozyreva et al 2020 *Psychological Science in the Public Interest* 105 and 108.

safeguard consumer privacy so that consumers are afforded effective statutory privacy protections in the digital age.[61]

1.3 Research Question

This study seeks to address the following research question:

Whether South Africa's regulatory framework on consumer privacy is adequate and appropriately enforced to ensure consumer protection in the digital age?

1.4 Aims and Objectives

1.4.1 Aims

The aims of the study include the overall goals that are relevant to achieving the objectives of the study. In this regard, the researcher seeks to:

a) Identify and critically discuss the strengths and weaknesses within South Africa's legal framework for regulating and enforcing consumer privacy rights.

b) Discuss the regulation and enforcement of consumer privacy in India and the European Union. This will be done to draw some lessons that could be adopted to strengthen South Africa's legal framework on the regulation and enforcement of consumer privacy.

c) Provide possible recommendations that could be adopted to enhance the regulation and enforcement of consumer privacy in South Africa.

1.4.2 Objectives

The objectives include the measures taken to achieve the overall aims of the study. In this regard, the researcher seeks to:

a) Trace the historical developments of the regulation and enforcement of consumer privacy in South Africa.

---

[61] Mtuze and Papadopoulos "Privacy and Data Protection" 376 and 377; Ooijen and Vrabec 2019 *Journal of Consumer Policy* 91 and 103-105.

b) Examine the adequacy of the current regulatory framework and enforcement approaches on consumer privacy in South Africa.

c) Provide a comparative analysis of the regulation and enforcement of consumer privacy by comparing South Africa's legal framework to India and the European Union.

d) Suggest recommendations for enhancing the legal framework for the regulation and enforcement of consumer privacy in the digital age in South Africa.

1.5 Rationale for the Study

Suppliers[62] and/or data controllers[63] oftentimes require consumers to provide their personal information to make use of and access various goods and services, especially in the digital market.[64] Consumers who provide data controllers and/or suppliers with their personal information potentially expose themselves to an innumerable amount of privacy threats.[65] This necessitates the critical analysis of South Africa's privacy framework to determine what privacy-related protections are available to consumers and the efficacy of such protections.

The internet serves a very important purpose in the modern era.[66] The Internet can result in the socio-economic improvement of South Africans by providing access to affordable goods and services, easily accessible educational material, health and wellbeing, and increasing economic activity.[67] The internet has also changed the overall way in which people interact with businesses and people.[68] Moreover, it enables access to a wider variety of goods and services, opportunities to learn, and

---

62 Section 1 of the *CPA;* A supplier is defined as a person who promotes or supplies goods or services.

63 Section 1 of the *POPIA;* A data controller is a person or entity that processes a consumer's personal information. For purposes of this mini-dissertation the term supplier and the term data controller are used interchangeably.

64 Nguyen et al 2023 *Applied Sciences* 1; Mtuze and Papadopoulos "Privacy and Data Protection" 322-325.

65 Duraiswami 2017 *Journal of Law and Cyber Warfare* 166; Nguyen et al 2023 *Applied Sciences* 2; Mtuze and Papadopoulos "Privacy and Data Protection" 307.

66 Nguyen et al 2023 *Applied Sciences* 1; Papadopoulos "An Introduction to Cyberlaw" 1.

67 Van Eeden and Barnard *Consumer Protection Law in South Africa* 553; Madone *Information Technology and People* 1; Pierce "Electronic Communications Regulation in South Africa" 36 and 37; Tladi and Papadopoulos "Consumer Protection in E-commerce" 75 and 78.

68 Schemer et al 2021*Journal of Computer-Mediated Communication* 1 and 4; Costa and Rodrigues 2022 *Review of Managerial Science* 2507.

the ability to communicate with people from all over the globe.[69] However, these benefits must not come at the cost of compromising consumers' privacy, as this goes against South African common law, the constitutional right to privacy,[70] the prescripts of the *CPA*'*s* intention of creating a fair and efficient marketplace,[71] and the *POPIA's* information processing principles.[72]

South Africa's comparatively underdeveloped privacy framework[73] and the overall weaknesses present in the South African privacy framework hinders the effective enforcement of privacy rights in South Africa. A comparative analysis of the European Union's and India's legal privacy framework aims to provide solutions to the identified weaknesses in South Africa's privacy framework. The reason and justification for using aspects of the European Union's privacy framework is that it is comparatively more established than South Africa's current privacy framework.[74] Additionally, the *General Data Protection Regulation*[75] is touted as the worldwide benchmark with regard to privacy legislation.[76] This results in a wealth of privacy-specific legal literature, and landmark court decisions that illustrate effective privacy protections available to consumers within the European Union's privacy framework.[77] Aspects of India's privacy framework are being analysed because India, like South Africa, is a developing nation.[78] This results in somewhat similar needs for sustainable socio-economic development and the privacy regulatory and enforcement framework needed to achieve a fair and equitable consumer marketplace.

---

69 Van Eeden and Barnard *Consumer Protection Law in South Africa* 553; Papadopoulos and Tladi "Consumer Protection in E-commerce" 75 and 78; Heyns and Kilbourn 2022 *Journal of Transport and Supply Chain Management* 2.

70 Section 14 of the *Constitution;* Currie and de Waal *Bill of Rights Handbook* 6th edition 294,295, and 309.

71 Section 3(1)(a) of the *CPA*; De Stadler and Eiselen "Section 3" *Protection Act* 3-3.

72 Section 4(1) of the *POPIA*; Papadopoulos and Mtuze "Privacy and Data Protection" 355 and 356.

73 Mtuze and Papadopoulos "Privacy and Data Protection" 322,325-342,348, and 349; Roos 2023 *THRHR* 4, 6, and 26.

74 Roos 2023 *THRHR* 4; Mtuze and Papadopoulos "Privacy and Data Protection" 325-338; Luisi 2022 *E-International Relations* 1.

75 *General Data Protection Regulation* (EU) 2016/679 (*GDPR).*

76 Roos 2023 *THRHR* 4; Mtuze and Papadopoulos "Privacy and Data Protection" 330; Luisi 2022 *E-International Relations* 1.

77 Marelli 2024 *International Data Privacy Law* 20; *IAB Europe v Gegevensbeschermingsautoriteit C-604/2*; *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* C-311/18; *Meta vs Bundeskartellamt Case* C-252/21.

78 Chaturvedi et al 2020 *Young Consumers* 400; Dhamija 2020 *South African Journal of Economics* 315; Marnewick and Bekker 2022 *Journal of Contemporary Management* 6.

The ubiquity of the internet brings both benefits and privacy-related risks.[79] While the internet has the potential to contribute to the socio-economic upliftment of South Africans, it also exposes consumers to numerous privacy risks that necessitate robust privacy protections. This research is important as it will provide a critical analysis of South Africa's privacy framework and identify the strengths and weaknesses of said privacy framework. By conducting a comparative analysis with the more established privacy framework of the European Union[80] and the similarly situated regulatory environment of India,[81] this study seeks to identify potential remedies that can be applied to South Africa's privacy framework. The insights gained from this research aim to improve South Africa's regulatory and enforcement framework, ensuring that the benefits of the internet[82] do not come at the cost of compromising consumer privacy.

1.6 Limitations of the Study

This study mainly focused on relevant privacy provisions contained in the *ECTA, the CPA, and the POPIA.* South African case law will be used to provide an overview of the development and enforcement of privacy rights in South Africa. Additionally, an assessment of current South African privacy enforcement bodies and their effectiveness in dealing with enforcing privacy rights in the ever-changing digital landscape[83] was part of the focus of this study. A comparative analysis between South Africa, India, and the EU will be conducted to identify relevant aspects to provide further improvements to the enforcement and protection of privacy rights in South Africa. This study did not focus on the historical development of India and the

---

79 Jones 2021 *Penn State Journal of Law and International Affairs* 220-222; Nadhom and Loskot 2018 *Journal Data Brief* 1922; Van Eeden and Barnard *Consumer Protection Law in South* 553; Madone *Information Technology and People* 1; Pierce "Electronic Communications Regulation in South Africa" 36 and 37; Tladi and Papadopoulos "Consumer Protection in E-commerce" 75 and 78; Nguyen et al 2023 *Applied Sciences* 2.

80 Roos 2023 *THRHR* 4; Mtuze and Papadopoulos "Privacy and Data Protection" 330; Luisi 2022 *E-International Relations* 1.

81 Chaturvedi et al 2020 *Young Consumers* 400; Dhamija 2020 *South African Journal of Economics* 315; Marnewick and Bekker 2022 *Journal of Contemporary Management* 6.

82 van Eeden and Barnard *Consumer Protection Law in South* 553; Madone *Information Technology and People* 1; Pierce "Electronic Communications Regulations in South Africa" 36 and 37; Tladi and Papadopoulos "Consumer Protection in E-commerce" 75 and 78.

83 Jones 2021 *Penn State* Journal *of Law and International Affairs* 220 and 221; Kozyreva et al 2020 *Psychological Science in the Public Interest* 105 and 108.

European Union's privacy laws. Due to the ever-changing digital landscape[84] this study will not discuss or focus on identifying consistent patterns of online privacy violations, as this would potentially date the findings of this research. This study will not be focussing on the detailed technicalities of how the internet functions and how personal information is collected.

1.7 Research Methodology

A desktop-based qualitative research methodology is used for this study. A desktop-based qualitative research methodology entails collecting, interpreting, applying and evaluating the material gathered to answer the research question.[85] Legislation, case law, and academic journal articles that mainly focus on privacy and privacy enforcement will serve as the main research material for this study. The findings from the abovementioned research material were used to illustrate areas in South African privacy law that may need improvement. The *Potchefstroom Electronic Law Journal* referencing style was followed in this study. The following research materials were utilised:

a) Primary and Secondary Sources

South African primary sources that will be used in this study are the *Interim Constitution*, the *Constitution,* the *CPA*, the *ECTA,* the *POPIA,* and relevant South African case law. Foreign primary sources that will be used in this study are the *GDPR*, relevant European Union case law, and the *Digital Personal Data Protection Act.*[86] The engagement and use of these sources are because they are the foundation of legal knowledge, enforcement and protection, and acquiring material from these sources provides an undiluted synopsis of privacy law.

The secondary sources used in this study will be journal articles and textbooks. These secondary sources will provide different perspectives, and different interpretations of

---

84 Syarah et al 2024 *International Journal of Religion* 7324; Verhoef et al 2019 *Journal of Business Research* 889 and 891.

85 William 2007 *Journal of Business and Economic Research* 67; Aspers and Corte 2019 *Qualitative Sociology* 142,147,and 155.

86 *Digital Personal Data Protection Act* 2023 (*DPDP Act*).

primary sources and assess the success of applicable privacy measures found in the enforcement of privacy rights contained in legislation.

b) Relevant Case Law

South African case law that shows the development of how privacy rights in South Africa are enforced will be used. South African case law will also be used to show the advantages and disadvantages of enforcing privacy rights through the courts. European Union and Indian case law will be used to compare how South African courts and European Union and Indian courts differ in their application and enforcement of privacy laws. Additionally, European Union and Indian case law will also illustrate industry-wide changes implemented on websites in response to punitive judgments.

c) Historical Analysis

The historical development of privacy rights and their enforcement in South Africa will be discussed in Chapter Two. This will provide a factual backdrop as to why privacy protection is important, and the need for well-developed privacy protections in the digital age.

1.8 Framework of Chapters and Outline of the Structure

Chapter One - Research Outline and Context

This chapter introduces the mini-dissertation topic. This chapter mentions the research problem, which is, a comparative analysis of the regulation and enforcement of consumer privacy in the digital age in South Africa, and the reasons behind selecting this topic. This chapter includes, the research question, aims and objectives, limitations of this study, and research methodology.

Chapter Two - Historical Development of Consumer Privacy Law in South Africa

This chapter provides an overview of the history of privacy enforcement in South Africa. This historical overview will start from 1993[87] up until the promulgation of the

[87] The year 1993 has been selected due to it being the year the *Jansen* case was decided. The *Jansen* case is the first relevant case that can be used when discussing consumer privacy.

POPIA. This discussion covers applicable privacy-related legislation and legislative enforcement of consumer privacy rights. Case law is used to illustrate how the consumer's right to privacy is enforced.

Chapter Three - The Regulation and Enforcement of Consumer Privacy in South Africa

This chapter focusses on South Africa's current legal privacy regime. Additionally, the strengths and weaknesses of South Africa's consumer privacy legal framework are identified. The reasons for identifying the strengths and weaknesses in South Africa's current legal framework is that it provides an overview of what the consumers' available privacy protections are and the efficacy of said protections.

Chapter Four- The Regulation of Consumer Privacy in the European Union and India

This chapter provides a discussion on the regulation of consumer privacy in the digital space in the European Union and India. It includes the identification of relevant privacy provisions, enforcement mechanisms, and case law that have had a global impact on consumer privacy protection, and draws lessons that could be applied to South Africa's legal privacy framework.

Chapter Five- Recommendations and Concluding Remarks

This chapter presents an overall conclusion and recommendations on how South Africa could enhance the regulation and enforcement of consumer privacy in the digital age.

CHAPTER TWO

HISTORICAL DEVELOPMENT OF CONSUMER PRIVACY LAW IN SOUTH AFRICA

2.1 Introduction

A discussion on the historical development of consumer privacy is essential as it highlights the regulatory and enforcement mechanisms before the promulgation of the South African *Constitution.*[88] An analysis of the development of consumer privacy before the promulgation of legislation containing specific privacy provisions will illustrate the strengths and weaknesses of South Africa's previous common law-dominated consumer privacy framework. Furthermore, South Africa's previous common law privacy framework still forms part of South Africa's current privacy framework[89] albeit in a less central manner due to the implementation of the *Protection of Personal Information Act.*[90] Moreover, examining the historical background will highlight the adaptability required for the effective enforcement of privacy rights in the constantly evolving digital landscape.[91]

This chapter presents a historical analysis of the development of consumer privacy law enforcement and regulation in South Africa. This historical overview focusses on the period before the current constitutional dispensation. This is done to examine how consumer privacy was regulated from 1993 to date to establish whether the developments around this area of law have been adequate for ensuring consumer protection over the years. Case law will be utilised to illustrate how the courts have been dealing with privacy rights and how these court judgements are relevant to the regulation and enforcement of consumer privacy.

---

88 Section 14 of the *Constitution of the Republic of South Africa,* 1996 (*Constitution*); Curie and de Waal *Bill of Rights Handbook* 36.

89 Preamble and section 14 of the *Constitution*; Currie and de Waal *Bill of Rights Handbook* 5; Preamble to the *POPIA*; Nagel et al *Commercial Law* 762 and 763; section 11 of the *Consumer Protection Act* 68 of 2008 (*CPA)*; section 43(1)(p) of the *Electronic Communications and Transaction Act* 25 of 2002 (*ECTA).;* Eiselen et al *"*Section 11" 11-5,6, and 7.

90 The preamble of *Protection of Personal Information Act* 4 of 2013 (*POPIA*); Mtuze and Papadopoulos "Privacy and Data Protection" 348 and 349; Eiselen et al "Section 11" 11-10,11, and 12; Nagel et al *Commercial Law* 375 and 376.

91 Jones 2021 *Penn State* Journal *of Law and International Affairs* 220 and 221; Kozyreva et al 2020 *Psychological Science in the Public Interest* 105 and 108.

2.2 The Regulation of Consumer Privacy under the Common Law

Prior to the promulgation of the *Constitution*, there were no easily identifiable privacy regulations contained in legislation, resulting in privacy rights being enforced via the common law, [92] due to the lack of legislation containing privacy provisions. Neethling correctly defines privacy as a state of a person's life in which an individual excludes certain aspects of their life from the public eye; it encompasses personal information that a person has chosen to keep private and wishes to remain unknown to others.[93] Applying Neethling's definition of privacy to consumer privacy would mean that consumers can control what personal information is shared with a supplier. To seek monetary redress through common law, a complainant must prove all the elements of a delict in a court of law.[94] South Africa's regulatory and enforcement privacy framework on privacy will be traced from 1993 when the *Jansen* case was decided.[95]

The historical development of consumer privacy rights will be traced from 1993.[96] In the *Jansen* case, the first defendant violated a consumer's privacy by disclosing their HIV status to a third party without the consumer's consent.[97] The consumer sought damages through the *actio iniuriarum,*[98] meaning all the elements of a delict would have to be proven to demonstrate a privacy violation.[99] This case is relevant to this discussion because it illustrated that a supplier's unauthorised disclosure of a consumer's personal information is a violation of a consumer's privacy rights. This indicates a supplier's duty with regard to a consumer's personal information. Additionally, this case illustrates the pitfalls of having to enforce privacy rights through

---

92 *Jansen van Vuuren and Another NNO v Kruger* [1993] 2 All SA 619 (A) para 8 (*Jansen* case); *Bernstein and Others v Bester NO and Others*(CCT23/95) [1996] ZACC 2 paras 68 and 69 (*Bernstein* case); Mtuze and Papadopoulos "Privacy and Data Protection" 312 and 313; McQuoid-Mason 1982 *CILSA* 135.

93 Neethling and Potgieter *Law of Delict* 370-372; *National Media Ltd v Jooste* 1996 (3) SA 262 (SCA) (*National Media* case) para 15.

94 *Jansen van Vuuren and Another NNO v Kruger* paras 9 and 17; *National Media* case para 16; Botha and Barnard *The Role and Responsibility of Suppliers in the Recall of Defective, Unsafe And Hazardous Consumer Products that Cause Harm 1*42; Barnard 2021 *International Journal on Consumer Practice* 45; Neethling and Potgieter *Law of Delict* 3-6,12-16, and 370-372; Mtuze and Papadopoulos "Privacy and Data Protection" 312; The delictual elements are conduct, wrongfulness, fault, causation, and damage.

95 *Jansen* case; Van Dokkum *South African Journal of Criminal Justice* 17.

96 *Jansen* case paras 9,10,14, and 43; Dancaster and Dancaster 1995 *SAMJ* 141.

97 *Jansen* case paras 1-9; Dancaster and Dancaster 1995 *SAMJ* 141.

98 *Jansen* case paras 8 and 9; Okpaluba 2015 *Actca Juridicia* 414.

99 *Jansen* case paras 8, and 17-19; Van Dokkum *South African Journal of Criminal Justice* 17.

the common law.[100] This is because they would have to prove all elements of a delict and then obtain damages through the civil courts.[101] Having to exclusively rely on the enforcement of privacy rights through the courts can be expensive and time-consuming.[102] The lack of a clearly defined and discernable privacy right could also unnecessarily extend court proceedings. This is due to the relevant parties having to establish what privacy entails, an endeavour that was fraught with challenges.[103] Thus, due to the lack of a clearly defined consumer privacy protection framework, the enforcement of consumer privacy was not as efficient or accessible as it could be.

In the *National Media* case,[104] the court addressed a privacy issue related to a respondent's control over the disclosure of their personal information to the public. The respondent agreed with the appellants in that the respondent would provide the appellants with details about their private life so that the respondent could publish said details in its magazine.[105] The respondent later withdrew their consent regarding the publication of details of their private life.[106] However, the appellants published details about the respondent's private life anyway.[107] The court found that the appellant had violated the respondent's privacy.[108] The court concluded that, although a person may provide another with their personal information, it is ultimately up to the person providing the personal information to decide what must happen with their personal information.[109] This case is relevant to consumer privacy as it underscores that a consumers' ability to control what happens to their personal information is a fundamental aspect of privacy. This implies that consumers are empowered to choose

---

100 Woker 2010 *Obiter* 223; Naudé & Eiselen "Introduction and Overview of the Consumer Protection Act" 1 and 11.

101 *Jansen* case paras 9 and 17; *National Media* case para 16; Botha and Barnard *De Serie Legenda Developments in Specific Contracts and Consumer Protection Law* 42; Barnard 2021 *International Journal on Consumer Practice* 45; Neethling and Potgieter *Law of Delict* 12-16, and 370-372; Mtuze and Papadopoulos "Privacy and Data Protection" 312.

102 *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* [2021] ZACC 3 para 49 (*AmaBhungane* case); Woker 2010 *Obiter* 231; Peté et al *Civil Procedure: A Practical Guide* 301.

103 *Bernstein* case para 65; *National Media* case paras 13-16; Mtuze and Papadopoulos "Privacy and Data Protection" 309 and 310; Frederick and Davids 1995 *Journal of South African Law* 479.

104 *National Media Ltd v Jooste* 1996 (3) SA 262 (SCA) paras 14 and 15 (*National Media* case); The respondent in this case was not a consumer. However, this case illustrates the court's interpretation and application of the concept of privacy.

105 *National Media* case paras 1-14; Okpaluba 2015 *Actca Juridicia* 412.

106 *National Media* case para 11; Okpaluba 2015 *Actca Juridicia* 412.

107 *National Media* case para 11; Neethling 2008 *SALJ* 40 and 41.

108 *National Media* case *Jooste* paras 16-18; Neethling 2008 *SALJ* 40 and 41.

109 *National Media* case paras 11, and 13-18; Neethling 2008 *SALJ* 40.

what happens with their personal information. Thus, the protection of consumer privacy rights includes the ability to control one's personal information. The strength of the common law's privacy framework is that it recognises that an individual's ability to choose what happens with their personal information is a component of the right to privacy.

The common law framework for the regulation and enforcement of privacy rights before the adoption of South Africa's current privacy framework was fraught with challenges.[110] Such challenges included the lack of a clear statutory framework on privacy rights and what those privacy rights entailed,[111] protracted and potentially complex legal proceedings,[112] and the exclusive reliance on potentially expensive civil court litigation.[113] As a result, privacy infringements had to be juridically assessed on a case-by-case basis. Nonetheless, a notable strength of the common law approach is its early acknowledgment that the right to privacy encompasses decisions about how personal information is withheld or shared.[114] Ultimately, the lack of an explicit right to privacy contained in legislation hampered the effectiveness of South Africa's privacy framework.

2.3 Privacy Under the Interim Constitution

Section 13 of the *Interim Constitution* was the first piece of legislation in South Africa that explicitly provided for the right to privacy.[115] Section 13 of the *Interim Constitution* stated that a person had the right to privacy which entailed that a person shall not be searched, that a person's private communications shall not be accessed, and that a person's private property should not be searched.[116] The *Interim Constitution* also provided for an aggrieved person with the right to approach a court to enforce their privacy rights.[117]

---

110 *Bernstein* case para 65; Mtuze and Papadopoulos "Privacy and Data Protection" 309.
111 See paras 2.2.1 and 2.2.2.
112 See paras 2.2.1 and 2.2.2.
113 *AmaBhungane* case para 49; Woker 2010 *Obiter* 231; Peté et al *Civil Procedure: A Practical Guide* 301.
114 *National Media* case paras 11, and 13-18.
115 Section 13 of the *Interim Constitution of South Africa Act* 200 of 1993 (*Interim Constitution)*; Rautenbach 2001 *Journal of South African Law* 120.
116 Section 13 of the *Interim Constitution*; Frederick and Davids 1995 *Journal of South African* 481 and 482.
117 Section 22 of the *Interim Constitution*; Asimow 1996 *American Journal of Comparative Law* 397.

The court in the *Bernstein v Bester* case remarked that the concept of what privacy specifically entails is unclear.[118] The court made use of the privacy clause in the interim Constitution.[119] The Interim *Constitution's* explicit mention of what privacy entails assisted the court when applying privacy rights.[120] The court found that in certain aspects of life, the right to privacy is strong, but if an individual places themselves in certain realms of life the strength of the right to privacy shrinks.[121] This case illustrated that the strength of the right to privacy depends on the particular aspect of life in which an individual is engaged. For consumers, this implies that when they buy or use certain goods or services, their privacy rights may not always be as strong as in other aspects of life. For example, if a consumer provides a supplier with their personal information in the course of a commercial transaction, the expectation of privacy may be reduced, especially if said personal information is needed for the fulfilment of the commercial transaction.

The *Interim Constitution* largely addressed the clarity issues associated with the concept of privacy rights under the common law.[122] By specifically stating what the right to privacy entails the contentious debate on what the concept of privacy entailed was mostly extinguished. Thus, a strength of the *Interim Constitution* is that it somewhat eliminated the contentious nature of what the concept of privacy entailed. However, the *Interim Constitution* did not make provision for out-of-court institutions.[123] This is a weakness because enforcing rights through the civil courts is expensive and thus out of reach for many consumers.[124] Additionally, the *Interim Constitution's* privacy provision was minimal with the relevant protections it offers to consumers in the digital age.

---

118 *Bernstein* case para 65; Rautenbach 2001 *Journal Of South African Law* 116; This was the first relevant case to this discussion that dealt with privacy rights under a piece of legislation that explicitly stated privacy rights.

119 Section 13 of the *Interim Constitution*; *Bernstein* case paras 44 and 57.

120 *Bernstein* case para 67; Papadopoulos 2009 *Obiter* 36.

121 *Bernstein* case para 67; Rautenbach 2001 *Journal Of South African Law* 116.

122 See paras 2.2.1 and 2.2.2.

123 Section 22 of the *Interim Constitution*; Asimow 1996 *American Journal of Comparative Law* 397.

124 *AmaBhungane* case para 49; *S v J* [2011] 2 All SA 299 (SCA) para 54; Woker 2019 *Stell LR* 104.

2.4 Conclusion

The historical development of consumer privacy in South Africa highlights the progression from the relatively unclear common law approach to a slightly more refined legislative framework in the form of the *Interim Constitution*. The initial exclusive reliance on the common law illustrated the challenges consumers faced when enforcing privacy rights due to the contentious nature of identifying and enforcing privacy rights.[125] These difficulties were compounded by the need to prove all delictual elements to succeed with a claim for damages from the civil courts.[126] The *Interim Constitution's* explicit mention of what the right to privacy entails was a step in the right direction as it made the regulation and enforcement of privacy rights slightly clearer.[127] However, South Africa's previous privacy regulatory and enforcement framework was not adequate in dealing with the protection of consumer privacy rights. The common law did not provide a clearly defined scope for the right to privacy, while the *Interim Constitution* lacked the detailed privacy provisions needed to address modern-day privacy demands and challenges.

In the next chapter, the researcher will focus on South Africa's current legal privacy regime regulated by the *Constitution,*[128] the *Electronic Communications and Transactions Act,*[129] the *Consumer Protection Act*,[130] and the *Protection of Personal Information Act.*[131] The strengths and weaknesses of South Africa's current consumer privacy legal framework will be discussed in detail. This will provide an overview of

---

125 *Bernstein* case para 65; Mtuze and Papadopoulos "Privacy and Data Protection" 309; Rautenbach 2001 *Journal Of South African Law* 116.

126 *Jansen van Vuuren and Another NNO v Kruger* paras 9 and 17; *National Media Ltd v Jooste* 1996(3) SA 262 (SCA) para 16; Botha and Barnard *De Serie Legenda Developments in Specific Contracts and Consumer Protection Law* 42; Barnard *International Journal on Consumer Practice* 2021 45; Neethling and *Potgieter Law of Delict* 12-16, and 370-372; Mtuze and Papadopoulos "Privacy and Data Protection" 312.

127 Section 13 of the *Interim Constitution; Bernstein* case paras 55 and 57.

128 Sections 1(a),7(1), and 14 of the *Constitution; Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* (CCT1/00) [2000] ZACC 12 para 9.

129 Section 43(1)(p) of the *Electronic Communications and Transactions Act* 25 of 2002 (*ECTA*)*;* Eiselen et al *"*Section 11" 11-10.

130 Sections 11 and 12 of the *Consumer Protection Act* 68 of 2008; *Kelter Presentations v Internet Service Providers'* [2014] JOL 31136 (GSJ) paras 7 and 79.

131 Preamble and section 2(a) of the *Protection of Personal Information Act* 4 of 2013 (*POPIA*)*;* Fritz 2021 *Constitutional Court Review* 1,2, and 5*;* Mtuze and Papadopoulos "Privacy and Data Protection" 348.

what the consumers' available privacy protections are and the efficacy of said protections in the digital age.

CHAPTER THREE

THE REGULATION AND ENFORCEMENT OF CONSUMER PRIVACY IN SOUTH AFRICA

3.1 Introduction

South Africa's legal framework on consumer privacy has evolved in recent years through the promulgation of legislation that specifically gives effect to the consumer's right to privacy. In particular, the *Constitution,*[132] the *Electronic Communications and Transactions Act,*[133] the *Consumer Protection Act,*[134] and the *Protection of Personal Information Act*[135] are the main pieces of legislation that primarily govern the consumer's right to privacy in South Africa. Notably, all these pieces of legislation were passed after 1996, and they give effect to the right to privacy as enshrined under the *Constitution*.[136] Without a doubt, the enactment of the *Constitution,* the *ECTA*, the *CPA* and the *POPIA* as pieces of legislation regulating issues of consumer privacy is a commendable development given that before the current statutory regime, issues of privacy were only regulated through the common law and the *Interim Constitution* as discussed in the previous chapter.

In this chapter, the researcher discusses the current regulatory and enforcement framework for consumer privacy in South Africa. Additionally, the strengths and weaknesses of South Africa's current consumer privacy regulatory and enforcement framework will be identified. The reasons for identifying the strengths and weaknesses in South Africa's current legal framework is that it will provide an overview of what the consumers' available privacy protections are and the efficacy of said protections.

---

132 *Constitution of the Republic of South Africa*, 1996 (*Constitution*); Currie and de Waal *Bill of Rights Handbook* 6th edition 36, 250, and 251.

133 Section 43(1)(p) of the *Electronic Communications and Transactions Act* 25 of 2002 (*ECTA*); Nagel et al *Commercial Law* 498.

134 Sections 11 and 12 of the *Consumer Protection Act* 68 of 2008 (*CPA)*; *Kelter Presentations v Internet Service Providers' [2014] JOL 31136 (GSJ)* paras 51,58,59, and 79 (*Kelter* case).

135 Preamble and section 2 of the *Protection of Personal Information Act* 4 of 2013 (*POPIA*); Nagel et al *Commercial Law* 763.

136 See section 14 of the *Constitution*; sections 11 and 12 of the *CPA*; sections 43(1)(p) and 43(5) of the *ECTA*; Tladi and Papadopoulos "Consumer Protection in E-commerce" 80,81,96,105, and 129; Eiselen et al "Section 11" 11-5,6,7,8,10, and 11; Preamble and section 2 of the *POPIA*; Mtuze and Papadopoulos "Privacy and Data Protection" 348; van Eeden and Barnard *Consumer Protection Law in South Africa* 567 and 568.

3.2 The Constitution

The *Constitution* is the supreme law of the land and any conduct that is in contravention of the provisions in the *Constitution* is deemed to be unconstitutional.[137] The *Constitution* was the first legal instrument in the democratic South Africa to explicitly introduce the right to privacy and outline what that right entails.[138] Section 14 of the Constitution grants everyone the right to privacy, which encompasses protection against the search or seizure of their person, property, or communications.[139] Section 34 of the *Constitution* provides everyone with the right to have a matter resolved by a court or any other relevant institution.[140] In light of this right, any aggrieved person may also approach a competent court to enforce their privacy rights.[141] The *Constitution* does not set out detailed privacy regulations tailored to the specific needs of consumer privacy protection in the digital age.[142]

In the *AmaBhungane Centre for Investigative Journalism v Minister of Justice and Correctional Services,* the Constitutional Court dealt with the constitutional right to privacy.[143] In this case, the applicants' personal information, more specifically their communications, was unlawfully accessed.[144] This access was, *inter* alia, made possible through the use of the *Regulation of Interception of Communications and Provision of Communication-Related Information Act.*[145] The Constitutional Court found that certain sections in the *Regulation of Interception of Communications and Provision of Communication-related Information Act*[146] were unconstitutional due to inadequate provisions ensuring that there are adequate security safeguards,

---

137 The preamble of the *Constitution*; Currie and de Waal *Bill of Rights Handbook* 5.

138 Section of the 14 of the *Constitution;* Phiri 2023 *Law, Democracy, and Development* 266.

139 Section 14 of the *Constitution;* Currie and de Waal *Bill of Rights Handbook* 294,295, and 309.

140 Section 34 of the *Constitution;* Currie and de Waal *Bill of Rights Handbook* 710 and 711.

141 Section 38 of the *Constitution*; Jephson 2014 *Constitutional Court Review* 286.

142 Specific privacy regulations will be discussed later on in this chapter.

143 Section 14 of the Constitution; *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* [2021] ZACC 3 para 2 (*AmaBhungane* case); Although the applicants in this case were not consumers this case illustrates how the Constitutional Court interprets and applies section 14 of the *Constitution*.

144 *AmaBhungane* case paras 13-17, and 38; Hungwe and Munoriyarwa 2024 *Statue Law Review* 7 and 8.

145 *AmaBhungane* case paras 13-22, and 24; *Regulation of Interception of Communications and Provision of Communication-Related Information Act* 70 of 2002 (*RICA)*; Hungwe and Munoriyarwa 2024 *Statue Law Review* 4.

146 Section 16(7), 17(6), 18(3)(a), 19(6), 20(6), 21(6), and 22(7) of the *Regulation of Interception of Communications and Provision of Communication-related Information Act* 70 of 2002 (*RICA)*; Papadopoulos "An Introduction to Cyberlaw" 4.

inadequate accountability procedures, and inadequate transparency mechanisms.[147] This case illustrates the advantage of having a legal instrument, the *Constitution,* that clearly mentions what the right to privacy is and what it entails.[148] Additionally, due to the supremacy of the *Constitution,* all privacy-related conduct is benchmarked against section 14 of the *Constitution.* This has a positive effect on consumers as it can potentially expedite court proceedings. This can be seen by the fact that the court did not have to identify what privacy specifically entails as that was already contained in section 14 of the *Constitution.*[149] This case is relevant to consumers in the digital age because it illustrates that suppliers who have inadequate security safeguards, a lack of transparency, and a lack of accountability violate constitutional privacy rights.

The promulgation of the *Constitution* marked a positive step forward from the common law by explicitly stating that everyone has the right to privacy and by outlining specific instances where this right applies.[150] This is due to the *Constitution* providing for a clearer regulatory and enforcement framework as the *Constitution* states what the right to privacy specifically entails.[151] Due to the *Constitution* being the supreme law of the land section 14 of the *Constitution* provides a benchmark with which all actions must comply.[152] However, the *Constitution* does not make provisions for specific privacy rights and obligations that are relevant to the consumer's right to privacy in the digital age. Specific privacy protections and out-of-court enforcement bodies were later established with the promulgation of the *ECTA,*[153] *the CPA*,[154] and the *POPIA*.[155]

3.3 The ECTA

The *ECTA* is the first piece of legislation that, *inter alia,* facilitates the creation of a safe and secure online environment.[156] The objectives of the *ECTA* include the creation of

147 *AmaBhungane* case paras 32,33,85-88, and 93-110; Basimanyane 2022 *African Journal of International and Comparative Law* 374.

148 Section 14 of the *Constitution*; Papadopoulos "An Introduction to Cyberlaw" 6; *AmaBhungane* case paras 2,55, and 188.

149 *AmaBhungane* case paras 2, and 55; section 14 of the *Constitution.*

150 Section 14 of the *Constitution; AmaBhungane* case paras 2, and 188.

151 Section 14 of the *Constitution; C*urrie and de Waal *Bill of Rights Handbook* 294 and 295.

152 Preamble and section 14 of the *Constitution;* Currie and de Waal *Bill of Rights Handbook* 5.

153 Section 43(p) of the *ECTA*; Tladi and Papadopoulos "Consumer Protection in E-commerce" 96.

154 Sections 11,12, and 69 of the *CPA*; Eiselen et al "Section 11" 11-6 and 10; van Heerden "Section 69" 69-1 and 2.

155 Preamble and section 39 of the *POPIA*; van Eeden and Barnard *Consumer Protection Law in South Africa* 568.

156 Section 2(1)(j) of the *ECTA*; Tladi and Papadopoulos "Consumer Protection in E-commerce" 82.

legal certainty regarding online activities, and ensuring that online transactions and communications are afforded the same protections as other methods of commerce.[157] Additionally, another objective of the *ECTA* is to foster a safe and secure online environment for consumers and suppliers.[158] The *ECTA* is relevant to consumer privacy in the digital age as it creates a clearly defined benchmark and framework for suppliers to comply with.

The *ECTA* is relevant to online consumer privacy protection as it applies to electronic transactions.[159] The *ECTA* requires suppliers to disclose their privacy policies regarding consumer's personal information.[160] Additionally, the privacy protections afforded to consumers in the *ECTA* entail informing consumers of the privacy protections available to them and requiring suppliers to ensure their facilities are capable of protecting consumers' personal information.[161] The *ECTA* requires suppliers to provide consumers with the opportunity to unsubscribe from receiving unsolicited direct marketing material.[162] This is relevant to consumer privacy in the digital age as it ensures that consumers are informed about suppliers' personal information processing policies and that those facilities are capable of securing consumers' personal information. Additionally, a supplier is required to inform a consumer on where and how they got the consumer's personal information.[163] A strength of the *ECTA* is that it enables consumers to make informed decisions regarding their personal information.[164] Another strength of the *ECTA* is that consumers are legally entitled to have adequate security safeguards that protect their personal information.[165] A key weakness of the *ECTA* is its lack of sufficient privacy protections that guard against modern-day privacy risks.[166]

---

157 Section 2(1)(e)(f)(j) of the *ECTA*; Tladi and Papadopoulos "Consumer Protection in E-commerce" 82.

158 Section 2(1)(j) of the *ECTA*; van Eeden and Barnard *Consumer Protection Law in South Africa* 55.

159 Section 4(1) of the *ECTA*; van Eeden and Barnard *Consumer Protection Law in South Africa* 556.

160 Section 43(1)(p) of the *ECTA*; Nagel et al *Commercial Law* 498.

161 Section 43(1)(p)(5) of the *ECTA;* Eiselen 2021 *TSAR* 448.

162 Section 45(1)(a) of the *ECTA*; section 1 of the *CPA*; Eiselen et al "Section 11" 11-10; Direct marketing is the act of advertising certain goods or services to consumers.

163 Section 45(1)(b) of the *ECTA*; Eiselen et al "Section 11" 11-10.

164 Section 43(1)(p)(5) of the *ECTA;* Eiselen 2021 *TSAR* 448; This is due to suppliers being required to inform consumers about its privacy policies.

165 Section 43(1)(p) of the *ECTA*; Nagel et al *Commercial Law* 498.

166 Sections 43(1)(p) of the *ECTA* and 45(1)(b) of the *ECTA*; Eiselen et al "Section 11" 11-10.

3.4 The CPA

The *CPA* aims to create and foster a fair and equitable consumer marketplace for South African consumers.[167] The *CPA* seeks to achieve this by establishing a consumer marketplace that is fair, responsible and accessible, prioritising the interests of the consumer.[168] The *CPA* aims to protect consumers from unconscionable conduct from suppliers.[169] Furthermore, the *CPA* aims to create positive socio-economic upliftment by ensuring responsible and informed consumer choice. This finds its relevance to consumer privacy protection in the digital age because it ensures that consumers can make educated decisions about how their personal information is processed. By promoting transparency and protecting consumers from unfair business practices, the *CPA* aims to create a safer digital environment.[170]

The *CPA's* privacy protections include empowering consumers to control whether or not they receive digital marketing material.[171] This control entails that consumers have the right to be left alone.[172] Consumers can activate their section 11(1) privacy rights by explicitly informing the supplier that they do not wish to receive any further direct marketing material from said supplier.[173] The *CPA* requires suppliers to implement mechanisms that allow consumers to stop receiving direct marketing materials.[174] A consumer can input their relevant personal information in a pre-emptive block registry and relevant suppliers must not contact said consumers for direct marketing purposes.[175] The administrator of said registry is prohibited from selling or sharing a consumer's personal information that is contained in the registry.[176]

In 2024, there was a proposed amendment to the *CPA* which aims to create additional requirements for direct marketers when advertising to consumers.[177] In terms of the proposed amendments, direct marketers are required to register annually on a

---

167 Section 3(1) of the *CPA*; Woker 2019 *Stell LR* 99.
168 Section 3(1)(a) of the *CPA*; Bauling and Nagtegaal *De Jure* 152.
169 Section 3(1)(d) of the *CPA;* Bauling and Nagtegaal *De Jure* 152.
170 Section 3 of the *CPA*; Woker 2019 *Stell LR* 99.
171 Section 11(1) of the *CPA*; Nagel et al *Commercial Law* 762 and 763.
172 Eiselen et al "Section" 11-13; *NM and Others v Smith and Others (Freedom of Expression Institute as Amicus Curiae)* 2007 (5) SA 250 (CC) para 32.
173 Section 11(2) of the *CPA*; Eiselen et al Section 11" 11-16.
174 Section 11(2)(4)(a) of the *CPA*; Eiselen et al *"*Section 11" 11-1,6,8, and 10.
175 Regulation 4(3)(a-c) of the *CPA;* Eiselen et al *"*Section 11" 11-2.
176 Regulation 4(3)(e) of the *CPA.*
177 Schedule 3(d) in GN R2798 in GG 51436 of 28 October 2024.

statutorily established opt-out registry.[178] Furthermore, direct marketers are, *inter alia,* required to remove personal information from consumers who have elected to pre-emptively block receiving of direct marketing material,[179] and not allowing direct marketers to contact consumers unless direct marketers have registered on the statutorily established opt-out registry.[180] The researcher submits that these proposed amendments represent a valuable step in protecting consumer privacy rights in the digital age. Requiring suppliers to register on a statutorily established opt-out registry creates an environment where those who disregard the wishes of consumers who have opted out of receiving direct marketing material can be more easily identified and sanctioned. Additionally, requiring suppliers to contact consumers only if they are registered on the statutorily established opt-out registry may compel suppliers to operate strictly within the privacy protections enshrined in the *CPA.*[181] This could have the impact of ensuring statutorily mandated privacy protections are more efficiently enforced due to the easy identification of recalcitrant suppliers and the increased accountability resulting from their inclusion in the official opt-out registry. Thus, the *CPA's* privacy protections entail providing consumers with the ability to restrict the receipt of direct marketing.[182]

Consumers can enforce their privacy rights contained in the *CPA* through redress institutions contained in the *CPA*, which are consumer ombuds with jurisdiction, the National Consumer Commission, and the National Consumer Tribunal.[183] Due to the interrelationship between the *ECTA,* the *CPA,* and the *POPIA*[184] privacy-related enforcement matters, in the context of the digital age, will in all likelihood be dealt with by the Information Regulator.[185] Thus, the researcher submits that a critical discussion

---

178 Schedule 3(d)(d)(7)(a) in GN R2798 in GG 51436 of 28 October 2024.
179 Schedule 3(d)(7)(h) in GN R2798 in GG 51436 of 28 October 2024.
180 Schedule 3(d)(7)(i) in GN R2798 in GG 51436 of 28 October 2024.
181 Section 11 of the *CPA*; Eiselen et al "Section 11" 11-1 and 2.
182 Section 11(1) of the *CPA*; Eiselen et al "Section 11" 11-1 and 2.
183 Section 69 of the *CPA;* Mupangavanhu 2012 *PER/PELJ* 322-331*;* van Heerden "Section 69" 69-1.
184 Section 2(9) of the *CPA*; Eiselen et al "Section 11" 11-6; Tladi and Papadopoulos "Consumer Protection in E-commerce" 81,95, 128, and 129-134.
185 Section 2(4) of the *POPIA*; *Chirwa v Transnet Ltd & others* [2008] 2 BLLR 97 (CC) (*Chirwa* case) paras 52 and 77; de Waal Current Allergy and Immunology 233; Section 2 of the *CPA* states that in matters where other pieces of legislation may provide better protection that piece of legislation should apply. The *POPIA* provides for a specialised privacy enforcement institution, so the enforcement of consumer privacy rights will likely be done through the Information Regulator and thus the enforcement framework enshrined in the *POPIA* will apply. In the *Chirwa* case, the court

on the enforcement institutions enshrined in the *CPA* would be irrelevant due to the Information Regulator being the institution that would primarily deal with privacy-related matters in the digital age.[186]

The *Kelter* case dealt with enforcing consumer privacy by way of assessing a supplier's adherence to section 11 of the *CPA.*[187] In this case, the applicant continued sending direct marketing materials to consumers despite consumers choosing not to receive direct marketing material.[188] In addition to this, the applicant failed to provide details on where they obtained the consumer's personal information from.[189] The court applied section 45 of the *ECTA,* sections 11 and 12 of the *CPA,* and section 69 of the *POPIA*,[190] and concluded that the supplier had infringed on consumers' right to privacy due to their non-compliance with the abovementioned privacy provisions.[191] This case demonstrates the strength of the *CPA* by showing that its privacy provisions are aligned with modern-day privacy requirements.[192] As illustrated in the *Kelter* case, the *CPA* can effectively and efficiently address common privacy violations,[193] specifically, those related to unsolicited direct marketing.

Thus, the right to privacy enshrined in the *CPA* consists of a consumer having the ability to control their receival of direct marketing material.[194] The case highlights the *CPA's* effectiveness in addressing modern privacy concerns, particularly in the realm of unsolicited direct marketing, demonstrating its relevance and strength in safeguarding consumers' privacy rights in the digital age. However, the *CPA* does not provide for specific privacy protections that take into account all privacy-related risks

indicated that if a specialised enforcement body is primarily tasked with specific areas of law, that body must be used when exercising one's rights.

186 Section 2(4) of the *POPIA*; *Chirwa* case paras 52 and 77; de Waal Current Allergy and Immunology 233.

187 Section 11 of the CPA; *Kelter* case paras 51,58,59, and 79.

188 *Kelter* case para 59.

189 *Kelter* case para 58.

190 *Kelter* case para 80; Section 69 of *POPIA*; Note that at the time *POPIA* was not signed into law, and section 69 at the time was section 66.

191 *Kelter Presentations v Internet Service Providers'* paras 68, and 76-83.

192 Jones 2021 *Penn State Journal of Law and International Affairs* 238; Boerman and Smit 2022 *Journal of Advertising* 60 and 62.

193 *Kelter* case para 52; Jáñez-Martino et al 2023 *Artificial Intelligence Review* 1146.

194 Sections 11 and 12 of the *CPA*; Eiselen et al "Section 11" 11-1 and 2.

present in the digital age.[195] This deficiency provided the backdrop for the promulgation of the *POPIA.*[196]

3.5 The POPIA

The purpose of the *POPIA* is to give effect to the constitutional right to privacy.[197] The *POPIA* aims to achieve this by regulating how consumers' personal information is processed.[198] This is done by establishing processing standards that comply with international standards,[199] such as the *General Data Protection Regulation.*[200] The *POPIA* also aims to provide rights and remedies to consumers who have experienced a privacy violation due to non-compliance with *POPIA* provisions.[201] These aims are to be achieved by the establishment of the Information Regulator.[202]

The *POPIA*'*s* eight processing principles are accountability, processing limitation, purpose specification, further process limitation, information quality, purpose specification, openness, security safeguards, and data subject participation.[203] These principles create a regulatory framework that suppliers must follow to protect the consumers' right to privacy.[204] The *POPIA* is also the current enforcement framework that deals with the consumers' right to privacy in the digital age by way of the creation of the Information Regulator.[205]

Regarding the receival of direct marketing material, the *POPIA* follows an opt-in regime.[206] Suppliers are only permitted to send direct marketing material to consumers if consumers have chosen to receive direct marketing material.[207] Additionally,

---

195 Eiselen 2021 *TSAR* 454; Tladi and Papadopoulos "Consumer Protection in E-commerce" 95.
196 Preamble and section 2 of the *POPIA*; Eiselen 2021 *TSAR* 448,449, 450, and 452.
197 Section 2(1) of the *POPIA*; *De Jager v Netcare Limited and Others* (42041/16) [2025] ZAGPPHC 141 para 7 (*De Jager* case).
198 Section 2(2) of the *POPIA*; Nagel et al *Commercial Law* 763.
199 Section 2(2) of the *POPIA*; Nagel et al *Commercial Law* 763.
200 *General Data Protection Regulation* 2016/679 (*GDPR*); Roos 2023 *THRHR* 4; Mtuze and Papadopoulos "Privacy and Data Protection" 330 and 348.
201 Section 2(3) of the *POPIA*; Schultz and Freedman 2023 *PER/PELJ* 18.
202 Section 2(4) of the *POPIA*; Papadopoulos 2022 *THRHR* 398.
203 Section 4(1) of the *POPIA*; van Eeden and Barnard *Consumer Protection Law in South Africa* 571-580.
204 Section 2 of the *POPIA*; van Eeden and Barnard *Consumer Protection Law in South Africa* 567 and 568.
205 Sections 2 and 39 of the *POPIA*; van Eeden and Barnard *Consumer Protection Law in South Africa* 568.
206 Section 69(1)(a) of the *POPIA*; Zenda et al 2020 *South African Computer Journal* 114.
207 Section 69(1)(a) of the *POPIA*; Zenda et al 2020 *South African Computer Journal* 114.

suppliers must provide consumers with their name relevant details of the sender and relevant details that consumers need in order to cease the direct marketing communications.[208]

The Information Regulator can receive complaints from consumers who have allegedly experienced a privacy-related violation due to non-compliance with the *POPIA.*[209] Upon completion of its investigation the Information Regulator can issue an enforcement notice which can require a supplier to stop engaging in prohibited conduct; require the supplier to take certain actions that will ensure its compliance with the *POPIA*; and stop processing personal information.[210] Additionally, the Information Regulator can impose an administrative fine of up to R10 million.[211] A supplier can apply to the Information Regulator for the variation of an enforcement notice[212] or approach a relevant High Court to set aside an enforcement notice.[213]

The *De Jager* legal matter addressed privacy rights in the context of the *POPIA*.[214] In this legal matter, the plaintiff received an operation from the defendant.[215] This operation went wrong and the defendant paid the plaintiff R4.5 million.[216] Months later the plaintiff amended their particulars of claim and demanded more money from the defendant.[217] The defendant then hired a private investigator to see whether or not the operation impacted the plaintiff's life and if the plaintiff's increased monetary claim from the defendant was justified.[218] The *De Jager* legal matter illustrated that certain processing principles of the *POPIA* may fall to the wayside if the purpose of the processing might necessitate such.[219] This is relevant to consumer privacy in the

---

208 Section 69(4) of the *POPIA*; sections 11 and 12 of the *CPA*; Shanapinda 2019 *The African Journal of Information and Communication* 10; It is worth mentioning that sections 11 and 12 of the *CPA* follows an opt-out approach regarding the sending of direct marketing consumers. Whereas, the *POPIA* follows an opt-in approach. It remains unclear as to which approach is to be followed in South Africa.

209 Section 74 of the *POPIA;* Bronstein 2022 *PER/PELJ* 4.

210 Section 95(1) of the *POPIA*; Swales et al 2022 *South African Journal of Science* 2.

211 Section109(1)(c) of the *POPIA*; Swales et al 2022 *South African Journal of Science* 2.

212 Section 96(1) of the *POPIA*.

213 Section 97(1) of the *POPIA*; Mtuze and Papadopoulos "Privacy and Data Protection" 372.

214 *De Jager v Netcare Limited and Others* (42041/16) [2025] ZAGPPHC 141 par 10; Although the parties in the matter were not consumers this legal matter finds relevance to this discussion. This case illustrates the interplay and relevance of the *POPIA's* provisions in everyday life.

215 *De Jager v Netcare Limited* [2024] JOL 65458 (GP) para 5.

216 *De Jager v Netcare Limited* [2024] JOL 65458 (GP) para 6.

217 *De Jager v Netcare Limited* [2024] JOL 65458 (GP) para 7.

218 *De Jager v Netcare Limited* [2024] JOL 65458 (GP) paras 1 and 9.

219 *De Jager v Netcare Limited and Others* (42041/16) [2025] ZAGPPHC 141 paras 23 and 27.

digital age because it illustrates that *POPIA's* privacy protections are not absolute and that a balance must be struck between the respective rights of all parties involved. The researcher submits that the *De Jager* legal matter is relevant to this mini-dissertation, as it illustrates how the enforcement of privacy rights under the *POPIA* is context-dependent, particularly where competing legal interests justify the limited application of certain *POPIA* processing principles.

The *POPIA* allows an aggrieved consumer to approach a civil court for monetary damages.[220] A consumer may institute a claim for damages on their behalf or the information Regulator may institute a claim for damages on behalf of the consumer.[221] This incentivises consumers to wait for the Information Regulator to complete its investigation as the Information Regulator may, on behalf of the consumer, institute a claim for damages, which by implication places the financial burden of court litigation on the Information Regulator.[222]

3.5.1 Strengths of the POPIA

The promulgation of the *POPIA* has brought South Africa's privacy framework more in line with the international gold standard in privacy protection.[223] This is due to the noticeable similarities between the *POPIA* and the *GDPR*, which is touted as the benchmark when it comes to privacy legislation.[224] For example, the *POPIA* and the *GDPR* processing principles establish a comparable privacy regulatory framework, outlining consumer protections and supplier obligations in data processing.[225] Furthermore, the various processing principles explicitly outline what is required of suppliers in the modern processing of personal information.[226] This clarity benefits courts by streamlining proceedings, as privacy-related requirements are explicitly outlined in *POPIA*, enabling relevant legal institutions to simply assess supplier compliance. Thus, the promulgation of the *POPIA* has provided South African

220 Section 99(1) of the *POPIA*; Mtuze and Papadopoulos "Privacy and Data Protection" 372.
221 Section 99(1) of the *POPIA;* Swales et al 2022 *South African Journal of Science* 2.
222 Section 99(1) of the *POPIA*; Schultz and Freedman 2023 *PER/PELJ* 20.
223 Roos 2023 *THRHR* 4; Mantelero 2021 *Computer Law and Security Review* 1; Mtuze and Papadopoulos "Privacy and Data Protection" 330 and 348.
224 Roos 2023 *THRHR* 4; Mantelero 2021 *Computer Law and Security Review* 1; Mtuze and Papadopoulos "Privacy and Data Protection" 330 and 348.
225 Section 4 of the *POPIA*; Article 1(a-f) of the *GDPR*; Roos 2023 *THRHR* 5-24.
226 Chapter 3 of the *POPIA*; Swales 2021 *South African Journal of Science* 2.

consumers with a piece of legislation that is in line with international privacy legislative standards and provisions and an explicit privacy framework that is in keeping with contemporary privacy demands.[227]

The promulgation of the *POPIA* has provided a more fleshed-out constitutional right to privacy.[228] The processing principles established in the *POPIA* have outlined clear obligations for suppliers to follow. Several weaknesses in the *POPIA* and South Africa's privacy framework limit the efficacy of South Africa's privacy framework in protecting the consumer's right to privacy in the digital age.

3.6 Weaknesses in South Africa's Regulatory Framework for Consumer Privacy

South Africa's privacy framework consists of various weaknesses that reduce its effectiveness. Some of these weaknesses include that the Information Regulator is not permitted to award damages to aggrieved consumers,[229] the imposition of a low administrative fine amount,[230] the lack of AI-specific legislation dealing with AI-related privacy risks,[231] and that the *POPIA* provides for no specific period when consumers have to be notified of a privacy breach.[232] Additional identified weaknesses include the fact that the *POPIA* does not require Information Officers who are employed/appointed by suppliers who process large amounts of sensitive personal information to be situated in South Africa,[233] and the lack of a statutorily mandated opt-out/opt-in registry in South Africa.[234] These weaknesses are isolated and outlined in more detail below.

---

227 Mtuze and Papadopoulos "Privacy and Data Protection" 348-351; Schultz and Freedman 2023 *PER/PELJ* 1; de Waal 2022 *Current Allergy and Immunology* 234.

228 Preamble to the *POPIA*; section 14 of the *Constitution*; Currie and de Waal *Bill of Rights Handbook* 5.

229 Section 99(1) of the *POPIA*; Mtuze and Papadopoulos "Privacy and Data Protection" 372.

230 Section 109(1)(c) of the *POPIA*; Swales 2022 *South African Journal of Science* 2.

231 "AI National Government Summit Discussion Document: South Africa's Artificial Intelligence(AI) Planning: Adoption of AI by Government 16" available at https://www.dcdt.gov.za/images/phocadownload/AI_Government_Summit/National_AI_Government_Summit_Discussion_Document.pdf; "South Africa National Artificial Intelligence Policy Framework 1,10" available at https://www.dcdt.gov.za/sa-national-ai-policy-framework/file/338-sa-national-ai-policy-framework.html; Gravett 2020 *South African Public Law* 19-23; van der Merwe 2023 *Obiter* 942.

232 Section 22(2) of the *POPIA*; Roos 2023 *THRHR* 20.

233 Section 55 of the *POPIA*; van Eeden and Barnard *Consumer Protection Law in South Africa* 578.

234 Schedule of 3 in GN R2798 in GG 51436 of 28 October 2024.

3.6.1 The Inability of the Information Regulator to Award Damages

The *POPIA* does not make provisions for the Information Regulator to make an award for damages to a consumer who has experienced an online privacy violation.[235] All online privacy-related matters fall under the scope of the *POPIA,*[236] and as such, the Information Regulator is the only out-of-court authority with jurisdiction in dealing with online privacy-related complaints.[237] Seeking financial redress exclusively through court litigation is a challenge because court litigation is expensive and time-consuming.[238]

Additionally, requiring consumers to seek monetary compensation for privacy violations through the civil courts limits the amount of consumers who can seek monetary redress from privacy violations. This is because of the expensive nature of court proceedings.[239] Section 99 of the *POPIA* provides for the Information Regulator to institute a claim for damages on behalf of a consumer.[240] However, the Information Regulator is not required to institute a claim for damages on behalf of a consumer.[241] Thus, requiring consumers to seek financial redress for privacy violations through the courts limits the number of consumers who can pursue such redress due to the high costs associated with litigation.[242]

Another weakness/issue arising from the Information Regulator's inability to award monetary damages directly to consumers is that it creates a time-consuming procedural hurdle. This follows that a consumer who wishes to obtain monetary damages for a privacy violation would in all likelihood have to submit a complaint to the Information Regulator, wait for the Information Regulator to conclude its investigation of the complaint, and then approach a court for monetary damages.[243]

---

235 Mtuze and Papadopoulos "Privacy and Data Protection" 372; Sections 40(1)(b-h) and 74(1) of the *POPIA*.

236 Section 3 of the *POPIA*; Mtuze and Papadopoulos "Privacy and Data Protection" 348 and 349.

237 Sections 39 and 40(1)(a-h) of the *POPIA*.

238 *AmaBhungane* case para 49; Woker 2010 *Obiter* 230; *S v Matomela* [1998] 2 All SA 1 (CK) paras 1 and 4; *Boxing South Africa v Qithi (Leave to Appeal)* [2022] JOL 56302 (LC) para 6; *Booi v Amathole District Municipality and Others* (CCT 119/20) [2021] ZACC 36*;* paras 51 and 52; Wald 1983 *Maryland Law Review* 770; Zeisel and Callahan 1963 *Harvard Law Review* 1616; Woker 2019 *Stell LR* 104.

239 *AmaBhungane* case para 49; Woker 2019 *Stell LR* 104; Woker 2010 *Obiter* 230.

240 Section 99(1) of the *POPIA*; Mtuze and Papadopoulos "Privacy and Data Protection" 372.

241 Section 99(1) of the *POPIA*; Papadopoulos 2022 *THRHR* 408*.*

242 *AmaBhungane case* para 49; Woker 2019 *Stell LR* 104; Woker 2010 *Obiter* 230.

243 Sections 74-80, and 99 of the *POPIA*; Papadopoulos 2022 *THRHR* 401.

There is currently no case law dealing with the matter of whether a consumer can approach a court directly instead of approaching the Information Regulator first, but there is case law that indicates that specialised out-of-court institutions should be approached first before approaching a court.[244] It would also be in the consumer's best financial interests to wait for the Information Regulator to complete its investigation as the Information Regulator may institute a claim on behalf of the consumer.[245] This creates an untenable situation due to the increased amount of time it will take for a consumer to obtain financial redress for a privacy violation. This extended process ultimately hinders timely access to justice for consumers, undermining the effectiveness of the *POPIA* in providing comprehensive and efficient protection for online privacy rights.

3.6.2 Low Administrative Fine Amount

Punitive fines can act as an effective deterrent against unlawful conduct.[246] The Information Regulator being able to only administer a fine amount of up to R10 million is too low and thus a weakness in South Africa's privacy framework.[247] The *POPIA* does make provision for the data controller to take into account the nature of the privacy infringement but the R10 million fine amount is too low.[248] It stands to reason that data controllers that gross billions of rands should be fined an amount that is in proportion to their revenue amount and the severity of the privacy infringement. Due to the low fine amount, data controllers with revenue in the billions, a fine of up to R10 million could amount to "the cost of doing business" and be an ineffective deterrent in engaging in prohibited conduct.[249] Therefore, the current R10 million fine under the *POPIA* is not large enough to deter data controllers with high revenues from infringing on the consumer's right to privacy.

---

244 *Chirwa* case para 77; *Joroy 4440 CC t/a UbuntuProcurement v Potgieter N.O. and Another* 2016 (3) SA 465 (FB) paras 6-10.

245 Section 99(1) of the *POPIA*; Roos 2023 *THRHR* 24.

246 Lund & Sarin 2021 *Texas Law Review* 292; Clinard 1982 *Michigan Law Review* 978; Feess et al 2018 *Journal of Economic Behavior and Organization* 59 and 71.

247 Section 109(1)(c) of the *POPIA*; Jones *Penn State Journal of Law and International Affairs* 235.

248 Section 109(3) of the *POPIA*; Jones *Penn State Journal of Law and International Affairs* 235.

249 Lund and Sarin 2021 *Texas Law Review* 291,292, and 341; Clinard 1982 *Michigan Law Review* 978.

3.6.3 Lack of Specific Legislation that Primarily Regulates AI

In the South African National Artificial Intelligence Policy Framework document, the government has identified the need for a specific and comprehensive AI regulatory framework due to the privacy risks associated with AI. In this policy framework document, the government has outlined that there must be a comprehensive policy framework that regulates AI in such a way as to curb against the negative privacy risks associated with AI.[250] If AI is used to process personal information it falls under the scope of the *POPIA*[251] and the *ECTA*,[252] but these Acts are not sufficient in dealing with the threat of AI as is evidenced by the rapidly changing nature of AI.[253] However, there is currently no AI-specific legislation that primarily deals with the privacy threats AI poses to consumers and is thus a weakness in South Africa's privacy framework. The government's explicit plans to implement a comprehensive AI regulatory framework evidences the inadequacies of South Africa's current privacy framework.[254]

The privacy threats AI may pose are its surveillance capabilities[255] and its degradation of the control aspect of a consumer's right to privacy.[256] AI's surveillance capabilities can result in it learning more about consumers than the consumers initially agreed to disclose.[257] The control aspect of the right to privacy can be negated by AI.[258]

---

250 "South Africa National Artificial Intelligence Policy Framework 1 and 3" available at https://www.dcdt.gov.za/sa-national-ai-policy-framework/file/338-sa-national-ai-policy-framework.html

251 Long title, preamble, sections 2, 3(1)(a)(ii), 3(4), 5(g), 69, and 71 of the *POPIA*; van der Merwe 2023 *Obiter* 942.

252 Sections 1 and 20 of the *ECTA*; Tladi and Papadopoulos "Consumer Protection in E-Commerce" 82.

253 Bartneck *An Introduction to Ethics in Robotics and AI* 36; Dwivedi et al 2023 *Technological Forecasting and Social Change* 2.

254 "AI National Government Summit Discussion Document: South Africa's Artificial intelligence (AI)Planning: Adoption of AI by Government 16" available at https://www.dcdt.gov.za/images/phocadownload/AI_Government_Summit/National_AI_Government_Summit_Discussion_Document.pdf; van der Merwe 2023 *Obiter* 942; "South Africa National Artificial Intelligence Policy Framework 1,3, and 10" available at https://www.dcdt.gov.za/sa-national-ai-policy-framework/file/338-sa-national-ai-policy-framework.html.

255 Hu and *Min International Journal of Hospitality Management* 2; Saheb 2023 *AI and Ethics* 369 and 374; Fontes 2022 et al *Technology in Society* 2 and 3.

256 Section 23-25 of the *POPIA*; *National Media Ltd v Jooste* 1996 (3) SA 262 (SCA) paras 11 and 13-18; Eliot and Soifer 2022 *Frontiers in Artificial Intelligence* 1; Bartneck *An Introduction to Ethics in Robotics and AI* 2 and 24.

257 Elliot and Soifer 2022 *Frontiers in Artificial Intelligence* 4 and 5; Hu and *Min International Journal of Hospitality Management* 2.

258 Martin and Zimmerman 2024 *Current Opinion in Psychology* 3-7; Elliot and Soifer 2022 *Frontiers in Artificial Intelligence* 5.

Consumers can typically control what personal information is available to suppliers,[259] but with AI, it can fill in the gaps of personal information the consumer has elected to not disclose.[260] Thus, eroding the control aspect of the right to privacy.

Thus, South Africa's privacy framework is inadequate in dealing with the privacy threats AI poses due to the lack of specific legislation that deals with the protection of consumer's personal information against the privacy threats of AI. AI-specific legislation is needed due to the new and unique privacy risks that AI might pose.

3.6.4 Lack of Time Period for Notification of Breach

The security safeguard processing principle in the *POPIA* requires suppliers to ensure that their facilities and procedures are capable of safeguarding consumer's personal information. In the event of a data breach suppliers must inform consumers within a reasonable time after the discovery of an alleged data breach.[261] This is a weakness because the concept of reasonableness does not provide for a specific time period in which consumers must be notified leaving the discretion of notification of a data breach with the data controller.[262] Consumers may not be provided with the opportunity to make immediate changes to lessen the negative impact of having their personal information unlawfully accessed. The *AmaBhungane* case illustrates the problematic nature of data controllers having the discretion to notify data subjects of instances where their personal information has been unlawfully accessed.[263] In this case, the data subjects had their personal information unlawfully accessed, and the *RICA* not providing for specific periods in which data subjects must be informed leaves instances where the data subjects could not take necessary steps to lessen the negative impact of having their personal information accessed.[264] Thus, by not providing a specific time period in which consumers must be made aware of data breaches, *POPIA* leaves

259 Sections 23-25 of the *POPIA*; Martin and Zimmerman 2024 *Current Opinion in Psychology.*
260 Elliot and Soifer 2022 *Frontiers in Artificial Intelligence* 5; Bartneck *An Introduction to Ethics in Robotics and AI* 41.
261 Section 22(2) of the *POPIA*; Mbonye and Moodley *South African Journal of Information Management* 6.
262 Section 22(2) of the *POPIA*; Mtuze and Papadopoulos "Privacy and Data Protection" 364.
263 *AmaBhungane* case paras 13-16.
264 *AmaBhungane* case paras 16, and 39-46.

consumers vulnerable to prolonged harm from unlawful access to their personal information.

3.6.5 Absence of Localisation Requirement for Information Officers

There is an explicit prohibition on the processing of special personal information,[265] unless, *inter alia,* the Information Regulator has approved the processing and the consumer has consented to the processing of special personal information.[266] The explicit prohibition on the processing of special information is due to the sensitive nature of the special personal information and the larger negative impact a potential data breach may have on an affected consumer.[267] Information Officers are usually one of the first touchpoints in instances of data-processing-related issues.[268] The *POPIA* does not require suppliers who process large quantities of special personal information to have Information Officers situated in South Africa. The lack of localisation with regard to the processing of special personal information is a weakness. This is a weakness because of the high-cost implications related to the service of relevant legal documents to individuals/entities in foreign countries, and the overall administrative obstacles associated with investigating and enforcing against entitles not situated within a country's borders.[269]

3.6.6 The Lack of a Statutorily Mandated an Opt-Out/Opt-in Registry

Section 11(3) of the *CPA* requires the establishment of an opt-out registry.[270] The lack of an opt-out/opt-in registry in terms of the *CPA* is a weakness because it results in the

---

265 Section 26 of the *POPIA*; Adams et al 2021 *South African Journal of Science* 2.

266 Section 27(1)(a)(2) of the *POPIA;* Adams et al 2021 *South African Journal of Science* 4.

267 *De Jager v Netcare Limited and Others* (42041/16) [2025] ZAGPPHC 141 para 14; Labreque et al 2021 *Journal of Business Research* 563; Pelteret and Ophoff 2016 *Informing Science: the International Journal of an Emerging Transdiscipline* 281,282, and 288; Olaniran and Williams *Platforms, Protests, and the Challenge of Networked Democracy* 79-86; Moseson et al 2022 *Plos One* 2,3, 12, and 13; The heightened risks consumers face from data breaches or unlawful access to their sensitive personal information are particularly evident when suppliers hold potentially incriminating special personal information. Additionally, in the *De Jager vs Netcare* matter it was remarked that the extra layer of protection afforded to the processing of special personal information is due to the increased risks associated with unauthorised processing of special personal information.

268 Section 10(2)(iv) of the *DPDP Act;* Sharma *International Journal of Law Management and Humanities* 1844.

269 Peté et al *Civil Procedure: A Practical Guide* 142 and 143; Mtuze “Electronic Contracts (E-contracts) and E-Commerce” 63 and 64.

270 Section 11(3) of the *CPA*; van Eeden and Barnard *Consumer Protection Law in South Africa* 559.

privacy rights enshrined in the *CPA* not being fully realised. Due to the absence of a statutorily mandated opt-out/opt-in registry[271] consumers privacy rights in terms of the *CPA*[272] are not fully realised. This is because consumers currently have to opt-out of direct marketing individually with each supplier,[273] rather than simply registering once on a central opt-out/opt-in registry that would theoretically prevent all unsolicited marketing communications.[274] Therefore, the lack of an operational opt-out/opt-in registry undermines the *CPA's* intent to provide consumers with a simple and effective mechanism for exercising their privacy rights.

3.7 Conclusion

South Africa's privacy framework, largely governed by the *POPIA*,[275] reflects significant advancements in aligning South Africa with international privacy standards.[276] The enactment of the *POPIA* has enhanced consumer privacy protections, ensuring they reflect modern privacy demands and global best practices.[277] Furthermore, the establishment and existence of an out-of-court institution like the Information Regulator,[278] provides accessible avenues for enforcing privacy rights without resorting to costly litigation.[279] The presence of specific privacy regulations across several legislative instruments such as the *POPIA*, the *CPA*, the *ECTA*, and the *Constitution*; ensures that privacy violations can be tackled with greater precision and efficiency.

Despite these strengths, there are notable weaknesses in South Africa's privacy framework. The inability of the Information Regulator to award damages directly to consumers,[280] resulting in financial redress only being available through costly court

---

271 Regulations 4(3) of the *CPA*; Schedule 3 in GN R2798 in GG 51436 of 28 October 2024.
272 Section 11 of the *CPA*; Eiselen et al "Section 11" 11-1.
273 Section 11(1)(2) of the *CPA*; van Eeden and Barnard *Consumer Protection Law in South Africa* 559.
274 McBride 2012 *BMC Medical Research Methodology* 4; "Annual Report of the Data Protection Commission 2007 20 and 48" available at https://www.dataprotection.ie/sites/default/files/uploads/2018-12/AR2007En.pdf.
275 Preamble and section 2 of the *POPIA;* Roos 2023 *THRHR* 3 and 4.
276 Roos 2023 *THRHR* 4; Mtuze and Papadopoulos "Privacy and Data Protection" 330.
277 Roos 2023 *THRHR* 4; Mtuze and Papadopoulos "Privacy and Data Protection" 330.
278 Sections 39 and 40 of the *POPIA;* Roos 2023 *THRHR* 23 and 24.
279 *AmaBhungane* case para 49; Woker 2010 *Obiter* 231; Peté et al *Civil Procedure: A Practical Guide* 301.
280 Section 99(1) of the *POPIA*; Roos 2023 *THRHR* 24.

litigation.[281] Additionally, the administrative fines imposed by the Information Regulator, capped at R10 million,[282] is not a sufficient deterrent for large corporations with significant financial resources. Another weakness in South Africa's privacy framework is the absence of specific legislation to address privacy threats posed by AI.[283] The lack of a prescribed timeframe for notifying consumers of data breaches leaves them vulnerable to the prolonged negative impacts of such violations.[284] The lack of an explicit provision for the localised processing of large quantities of sensitive personal information. Finally, the lack of a statutorily mandated opt-out/opt-in registry in South Africa is a weakness.[285] Addressing these weaknesses would strengthen South Africa's privacy framework and ensure that it provides comprehensive, timely, and effective protection for consumers' privacy rights in the digital age.

The next chapter will provide a discussion of the regulation of consumer privacy in India and the European Union. This will be done to draw lessons that South Africa could apply to its privacy legal framework on consumer privacy.

281 *AmaBhungane* case para 49; Woker 2010 *Obiter* 231; Peté et al *Civil Procedure: A Practical Guide* 301.

282 Section 109(1)(c) of the *POPIA;* Mtuze and Papadopoulos "Privacy and Data Protection" 373.

283 Elliot and Soifer 2022 *Frontiers in Artificial Intelligence* 4; Saheb 2023 *AI and Ethics* 369 and 374; Elliot and Soifer 2022 *Frontiers in Artificial Intelligence* 1; Bartneck *An Introduction to Ethics in Robotics and AI* 2 and 24.

284 Section 22(2) of the *POPIA*; Mtuze and Papadopoulos "Privacy and Data Protection" 364.

285 Schedule 3 in GN R2798 in GG 51436 of 28 October 2024.

CHAPTER FOUR

THE REGULATION OF CONSUMER PRIVACY IN THE EUROPEAN UNION AND INDIA

4.1 Introduction

The weaknesses in South Africa's privacy regulatory framework, as discussed in the previous chapter, hinder the effective enforcement and regulation of consumer rights in the digital age. To address these weaknesses in the South African regulatory framework for online privacy, potential solutions may be found through a comparative analysis of relevant European and Indian privacy legislation.

Comparing South Africa's privacy framework to the European Union's (EU) and India's framework may identify regulatory improvements suited to South Africa's regulatory framework. The *General Data Protection Regulation*[286] is the global standard when it comes to privacy regulation.[287] Due to the *GDPR* being touted as the benchmark for privacy protection,[288] benchmarking South Africa's privacy framework against the *GDPR* is needed to identify relevant provisions in the *GDPR* that may address the weaknesses in South Africa's privacy framework. South Africa and India are both developing nations,[289] which results in there being comparable socio-economic conditions between the two nations. This comparable socio-economic setting results in similar privacy-related protections that are needed to create and sustain an equitable consumer privacy landscape. This is relevant because it can indicate the feasibility of incorporating the strengths of India's privacy framework into South Africa's privacy framework due to the comparable socio-economic setting present in both countries.[290]

---

286 *General Data Protection Regulation* 2016/679 (*GDPR*).

287 Roos 2023 *THRHR* 4; Mtuze and Papadopoulos "Privacy and Data Protection" 330; Luisi 2022 *E-International Relations* 1.

288 Roos 2023 *THRHR* 4; Mtuze and Papadopoulos "Privacy and Data Protection" 330; Luisi 2022 *E-International Relations* 1.

289 Chaturvedi et al 2020 *Young Consumers* 400; Dhamija 2020 *South African Journal of Economics* 315; Marnewick and Bekker 2022 *Journal of Contemporary Management* 6.

290 Chaturvedi et al 2020 *Young Consumers* 400; Dhamija 2020 *South African Journal of Economics* 315; Marnewick and Bekker 2022 *Journal of Contemporary Management* 6.

In this chapter, the researcher will provide a brief overview of the EU and India's privacy frameworks. The discussion of the relevant provisions in the EU and India's privacy framework will be done to draw comparable lessons for South Africa to enhance its regulatory framework for consumer privacy. The strengths of said privacy frameworks will be discussed and applied to the identified weaknesses in South Africa's privacy framework.

4.2 Overview of the Regulation of Consumer Privacy in the EU

The regulation of consumers' personal information is regulated by the *GDPR* in the EU.[291] The aim of the *GDPR* is to protect consumer's personal information by way of establishing rules and standards that suppliers must comply with when processing personal information.[292] The rules and standards of the *GDPR* must be followed when suppliers outside the borders of the EU process EU consumers' personal information.[293]

Due to the privacy-related risks imposed by Artificial Intelligence (AI),[294] the EU has also adopted a comprehensive *European Union Artificial Intelligence Act* (*EU AI Act*)[295] which will be discussed in this chapter. The need to compare South Africa's privacy-related AI protection against the EU's legislative framework that deals with the privacy-related threats that AI may pose is necessary. This comparison may provide a foundation for a more fleshed-out approach to combating the risks posed by AI.

4.2.1 The GDPR

The *GDPR* is relevant to EU consumers' online privacy as it mandates that suppliers adhere to specific principles when processing personal information.[296] Some of these principles include lawfulness of processing, collection of personal information for a specific purpose, and collection of the bare minimum amount of personal information (data minimisation).[297] Additional processing principles include ensuring the accuracy

---

291 Article 1(2) of the *GDPR*; Issaoui et al 2023 *Future Business Journal* 2.
292 Article 1(1) of the *GDPR*; De-Yolande et al 2023 *Voice of the Publisher* 334.
293 Article 3 of the *GDPR*; de Hart and Czerniawski 2016 *International Data Privacy Law* 230.
294 See para 3.6.3.
295 *European Union Artificial Intelligence Act* 2024/1689 (*EU AI Act)*; Molnar 2024 *Regional Law Review* 155.
296 Article 5 of the *GDPR;* Roos 2023 *THRHR* 25 and 26.
297 Article 5(a-c) of the *GDPR*; Roos 2023 *THRHR* 25 and 26.

of personal information, limiting the retention of personal information to only as long as necessary, maintaining accountability, and implementing security safeguards.[298] The influence the *GDPR* has had on the *POPIA* is clear, as the *POPIA's* eight processing principles[299] are strikingly similar to the principles processing principles found in the *GDPR*.

The *GDPR* requires each member state to set up a Supervisory Authority that is tasked with ensuring compliance with the *GDPR* and holding suppliers accountable for instances of privacy violations.[300] A Supervisory Authority may require suppliers who are not in compliance to, *inter alia,* comply with the *GDPR's* provisions, comply with a relevant request made by a consumer, and to temporarily or permanently stop processing personal information, or institute a punitive fine.[301]

The *GDPR* makes provision for the use of a punitive fine against suppliers who breach *GDPR* provisions.[302] An EU member state's Supervisory Authority may impose a fine amount of up to €10 million or two per cent of a supplier's annual turnover in the previous year, whichever is higher.[303] If a supplier breaches certain provisions of the *GDPR* a supplier may be fined €20 million or four per cent of their annual turnover in the previous, whichever is higher.[304]

Article 58(2) of the *GDPR* does not grant an EU member state's Supervisory Authority the ability to make an award for damages to an aggrieved consumer.[305] However, the *GDPR* does require relevant not-for-profit consumer protection institutions to institute

---

298 Article 5(c-f) of the *GDPR*; Mtuze and Papadopoulos "Privacy and Data Protection" 331.

299 Section 4(1) of the *POPIA*; van Eeden and Barnard *Consumer Protection Law in South Africa* 571-580; Roos 2023 *THRHR* 25 and 26.

300 Article 51 of the *GDPR*; Klar 2020 *Hastings Science and Technology Law Journal* 51.

301 Article 58(2) of the *GDPR*; Hoofnagle et al 2019 *Information Technology & Technology Law* 66.

302 Article 83(4) of the *GDPR*; Hoofnagle et al 2019 *Information Technology & Technology Law* 66.

303 Article 83(4) of the *GDPR*; Vandezande 2019 *International Journal for the Data Protection Officer, and Privacy Counsel* 17.

304 Article 83(5) of the *GDPR*; Vandezande 2019 *International Journal for the Data Protection Officer, and Privacy Counsel* 17; Alongside the *GDPR*, France has its own privacy regulation the *French Data Protection Act* No 78-17 of 1978; The French Supervisory Authority, the National Commission for Information Technology and Civil Liberties (CNIL), tasked with enforcing *GDPR* and *FDPA* provisions can impose a € 100 000 for every day a data controller does not comply with an it has made.

305 Article 58(2) of the *GDPR*; Solove and Schwartz EU *Data Protection and the GDPR:[Connected EBook]* 36.

a claim on behalf of aggrieved consumers who have suffered monetary loss due to non-compliance with *GDPR* provisions.[306]

Included in the security safeguard processing principle enshrined in the *GDPR*, suppliers are required to notify consumers of data breaches.[307] Suppliers must notify consumers within a maximum period of 72 hours.

From a comparative perspective, it is clear that the adoption of the *GDPR* was a commendable development in the regulation of consumer privacy. This follows the incorporation of clear measures such as the establishment of the Supervisory Authority, a punitive fine, awarding of damages and a timeframe for notifying consumers of data breaches. These progressive aspects will be further discussed and analysed below to outline how they could be considered as some of the strengths in the regulatory framework for consumer privacy in the EU which could be adopted in South Africa.

4.2.2 The EU AI ACT

AI presents various risks and benefits to society,[308] making a comprehensive regulatory framework is essential to maximise the advantages of AI and minimise the disadvantages of AI.[309] A comprehensive AI regulatory framework was adopted to promote innovation whilst also protecting fundamental human rights.[310] The *EU AI Act* classifies AI into three categories based on the AI's capability of infringing fundamental human rights, one of which is privacy.[311] The categories are unacceptable risk, high risk, and minimal risk.[312] AI systems that pose an unacceptable risk to fundamental human rights are banned in the EU.[313] AI systems that can pose a high risk to fundamental human rights must undergo an assessment in order for it to be used in

306 Article 80(1) of the *GDPR;* Solove and Schwartz *EU Data Protection and the GDPR: [Connected EBook]* 207.
307 Article 33(1) of the *GDPR*; De-Yolande et al 2023 *Voice of the Publisher* 336.
308 Sharma 2024 *Futures* 1; Ahmad et al 2023 Humanities and Social Sciences Communications 2.
309 Boura *Athens Journal Law* 386; Henson 2024 *Missouri Law Review* 850.
310 Recital 1 of the *EU AI* Act; Molnar 2024 *Regional Law Review* 158.
311 Recital 48 of the *EU AI Act*; Olimid et al 2024 *Access to Justice in Eastern Europe* 63.
312 Aboy et al 2024 *NPJ Digital Medicine* 3; Articles 5(1-5), 6(1)(2), and 27(1) of the *EU AI Act.*
313 Articles 5(1-5) of the *EU AI Act*; Aboy et al 2024 *NPJ Digital Medicine* 3.

the EU.[314] The minimal risk category carries with it little to no risk to privacy rights.[315] AI systems falling under the minimal risk category are recommended to follow principles of non-discrimination, fairness, and human oversight.[316] This tiered approach aims to ensure that AI technologies are regulated proportionately to their potential impact on privacy rights.

The EU Commission alongside the EU AI Board ensures compliance with the provisions of the *EU AI Act*.[317] The EU AI Board provides guidance and sets standards that must be complied with by relevant parties that use AI.[318] The EU Commission can institute a punitive administrative fine of up to €35 million or 7% of a company's annual turnover for non-compliance with provisions of the *EU AI Act*.[319] This ensures that fines are proportionate to the size of the company and the severity of its non-compliance with the *EU AI Act.*[320]

4.2.3 Strengths of the EU Privacy Framework

The EU privacy framework has strengths that when put up against South Africa's privacy framework illustrate the weaknesses present in South Africa's privacy framework. In particular, some of the strengths of the EU privacy framework include a higher administrative fine amount in the EU privacy framework, the requirement for not-for-profit institutions to institute a claim for damages on behalf of the consumer, an explicit requirement that suppliers must notify consumers within 72 hours of becoming aware of a data breach, and AI-specific legislation. These strengths are discussed below.

---

314 Articles 6(1)(2) and 27(1) of the *EU AI Act*; Recital 48 of the *EU AI Act*; Olimid et al 2024 *Access to Justice in Eastern Europe* 63.

315 Article 6(3) of the *EU AI* Act; van Kolfschooten and van *Oirscho* 2024 *Health Policy* 2.

316 Recital 27 of the *EU AI Act*; Olimid et al 2024 *Access to Justice in Eastern Europe* 9.

317 Articles 65, 66, and 99 of the *EU AI Act*; Guadamuz *the Journal of World Intellectual Property* 3; Wachter *Yale Journal of Law & Technology* 685.

318 Article 66 of the *EU AI Act*; van Kolfschooten and van *Oirscho* 2024 *Health* 4.

319 Article 99(3) of the *EU AI Act*; Wachter *Yale Journal of Law & Technology* 693.

320 Article 99(1) of the *EU AI Act*; Wachter *Yale Journal of Law & Technology* 693.

4.2.3.1 A Higher Fine Amount

Non-compliance with privacy regulations can cause societal harm,[321] thus it is imperative that fines adequately punish responsible parties and the fine amount reflects the severity of the breach and the financial capacity of the responsible parties.[322] The efficacy of fines that are somewhat in proportion to the offence and the turnover of the guilty party can be seen in the fine the National Commission for Information Technology and Civil Liberties (CNIL) fine imposed on Google.[323] The CNIL instituted a €50 million fine against Google for contravention of the *GDPR's* provisions.[324] Due to Google's large user base and the societal implications of Google not adhering to necessary privacy provisions a fine of €50 million is somewhat more in line with the gravity of the offence[325]

A strength of the *GDPR* and the *French Data Protection Act*[326] is that their fines are more proportionate to a supplier's revenue, providing a more effective deterrent against prohibited behaviour.[327] The *GDPR* compared to South Africa's *POPIA*, allows for fine amounts that are more in proportion to the negative consequences attributed to violations of privacy obligations and more in proportion to a responsible party's financial position. Furthermore, the CNIL's authority to impose a penalty of €100,000 per day on suppliers who fail to comply with orders adds significant pressure for timely compliance with relevant privacy provisions.[328] This may create a stronger incentive

---

321 See *Employees' Retirement System of Rhode Island, et. al. v. Mark Zuckerberg, et al. and City of Warwick Retirement System et. al.* 2021-0617-JRS: paras 186,190, and 191; Ruohonen and Hjerppe 2021 *Information Systems* 6; See *United States of America v Facebook Inc.* 456 F. Supp. 3d 105 (D.D.C. 2020) paras 118-125; Hu 2020 *Big Data and Society* 1-3.

322 *United States of America v Facebook Inc.* para 120; Lund and Sarin 2021 *Texas Law Review* 291 and 292; Vandezande 2019 *International Journal for the Data Protection Officer, and Privacy Counsel* 18.

323 Vandezande 2019 *International Journal for the Data Protection Officer, and Privacy Counsel* 18; Tambou 2019 *European Data Protection Law Review* 80; De-Yolande et al 2023 *Voice of the Publisher* 335.

324 Vandezande 2019 *International Journal for the Data Protection Officer, and Privacy Counsel* 18; Tambou 2019 *European Data Protection Law Review* 81; Google was found to have obtained invalid consent from users, a lack of transparency, and an inadequate amount of information being presented to consumers for them to make an informed choice.

325 Tambou 2019 *European Data Protection Law Review* 82; Vandezande 2019 *International Journal for the Data Protection Officer, and Privacy Counsel* 18.

326 *French Data Protection Act* No 78-17 of 1978 (*FDPA).*

327 Lund and Sarin 2021 *Texas Law Review* 292; Clinard 1982 *Michigan Law Review* 978; Feess et al 2018 *Journal of Economic Behavior and Organization* 59 and 71.

328 Article 20(III)(2) of the *FDPA*; Samonte *European Papers-A Journal on Law and Integration* 2019 841.

for suppliers to swiftly implement corrective measures and adhere to privacy obligations. Whereas, the *POPIA* does not contain any provision that explicitly mentions the Information Regulator being able to impose a daily financial penalty on suppliers who do not timeously implement its findings.

4.2.3.2 The Requirement for Not-For-Profit Institutions to Institute a Claim for Damages on Behalf of the Consumer

Like the Information Regulator in the *POPIA*,[329] the *GDPR* does not grant an EU member state's Supervisory Authority the ability to make an award for damages to an aggrieved consumer.[330] However, a strength of the *GDPR* is that it requires relevant not-for-profit consumer protection institutions to institute a claim on behalf of aggrieved consumers who have suffered monetary loss due to non-compliance with *GDPR* provisions.[331] This is advantageous because it alleviates the financial burden on consumers seeking damages for privacy infringements.[332] This is because the relevant consumer protection institution would likely bear the costs associated with civil litigation, rather than the consumer. Whereas, the *POPIA* does not provide consumers with the right to mandate a not-for-profit consumer protection institution to institute an action for damage on behalf of an aggrieved consumer. This results in a consumer potentially having to pay exorbitant litigation fees to seek monetary relief for a violation of their privacy rights.[333]

4.2.3.3 Determinable Notification Period

The *GDPR* mandates that suppliers notify an EU member state's Supervisory Authority within 72 hours of discovering a data breach.[334] Whereas, the *POPIA* requires suppliers to notify the Information Regulator as soon as reasonably possible.[335] The

---

329 Section 99(1) of the *POPIA;* Mtuze and Papadopoulos "Privacy and Data Protection" 372.

330 Article 58(2) of the *GDPR*; Solove and Schwartz EU *Data Protection and the GDPR: [Connected EBook]* 36.

331 Article 80(1) of the *GDPR;* Solove and Schwartz *EU Data Protection and the GDPR: [Connected EBook]* 207.

332 Woker 2010 *Obiter* 231; *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* [2021] ZACC 3 para 49 (*AmaBhungane* case); Peté et al *Civil Procedure: A Practical Guide* 301.

333 Woker 2010 *Obiter* 231; *AmaBhungane* case para 49; Peté et al *Civil Procedure: A Practical Guide* 301.

334 Article 33(1) of the *GDPR*; De-Yolande 2023 *Voice of the Publisher* 356.

335 Section 22(1)(2) of the *POPIA*; van Eeden and Barnard *Consumer Protection Law in South Africa Act* 577.

stipulated 72-hour notification period is a strength because it creates a determinable time frame that suppliers must follow.[336] By contrast, the *POPIA's* 'as soon as reasonably possible' timeframe can create ambiguity, as reasonableness is a flexible concept.[337] Thus, the *GDPR's* 72-hour time frame eliminates ambiguity and delays in reporting, ensuring that data breaches are promptly addressed and reducing the potential harm to affected consumers.

4.2.3.4 Adoption of a Comprehensive AI Regulatory Framework

Another strength of the EU privacy framework is the adoption of a comprehensive *AI Act*. The EU has a dedicated piece of legislation specifically designed to address the privacy risks posed by AI systems, offering more robust protection for consumers. Unlike the EU, South Africa does not have any AI-specific legislation.[338] The South African government has acknowledged the need for a comprehensive regularity framework that is needed to specifically deal with the privacy risks AI may pose.[339] But until South Africa implements AI-specific legislation the current privacy threats that AI systems pose are largely unregulated in South Africa. Currently, the *ECTA*[340] and the *POPIA*[341] is the only legislation in South Africa that addresses AI-related privacy threats, but the EU's introduction of AI-specific legislation demonstrates the necessity of a dedicated legal framework.

---

336 Article 33(1) of the *GDPR*; Borgesius et al 2023 *Scripted* 360.

337 Section 22(1)(2) of the *POPIA;* Neethling and Potgieter *Law of Delict* 214 and 215; Ahmed 2019 *PER/PELJ* 2, and 6-9.

338 "AI National Government Summit Discussion Document: South Africa's Artificial Intelligence(AI) Planning: Adoption of AI by Government 16" available at https://www.dcdt.gov.za/images/phocadownload/AI_Government_Summit/National_AI_Government_Summit_Discussion_Document.pdf; "South Africa National Artificial Intelligence Policy Framework 1 and 10" available at https://www.dcdt.gov.za/sa-national-ai-policy-framework/file/338-sa-national-ai-policy-framework.html.

339 "AI National Government Summit Discussion Document: South Africa's Artificial Intelligence(AI) Planning: Adoption of AI by Government 16,22, and 41" available at https://www.dcdt.gov.za/images/phocadownload/AI_Government_Summit/National_AI_Government_Summit_Discussion_Document.pdf; "South Africa National Artificial Intelligence Policy Framework 1,3,10" available at https://www.dcdt.gov.za/sa-national-ai-policy-framework/file/338-sa-national-ai-policy-framework.html.

340 Sections 1 and 20 of the *ECTA*; Tladi and Papadopoulos "Consumer Protection in E-Commerce" 82.

341 Long title, preamble, sections 2, 3(1)(a)(ii), 3(4), 5(g), 69, and 71 of the *POPIA*; van der Merwe 2023 *Obiter* 942.

4.3 Overview of India's Consumer Privacy Framework

4.3.1 Digital Personal Data Protection Act

In 2023, India passed the *Digital Personal Data Protection* Act,[342] which governs India's privacy framework.[343] The aim of the *DPDP Act* is to establish requirements that suppliers must adhere to in order to protect consumers' personal information. Some of the conditions for processing personal information under the *DPDP* Act include obtaining proper consent from a consumer[344] and ensuring that processing serves a legitimate purpose.[345] Additionally, another condition is that suppliers must erase consumers' personal information as soon as the consent for processing their personal information has been withdrawn.[346] Another condition for lawful processing is that suppliers must implement adequate security safeguards to protect consumers' personal information.[347] The *DPDP Act* also requires suppliers to establish procedures for addressing consumers' data processing-related grievances.[348] The Data Protection Board (DPB) is the institution tasked with ensuring and enforcing compliance with the *DPDP Act*.[349]

The DPB can take various actions to ensure compliance with the provisions *DPDP Act* and additionally, the *DPDP Act* requires some suppliers[350] to appoint Information Officers who are based in India.[351] The *DPDP Act* requires a supplier to erase all of a consumer's personal information.[352] Upon becoming aware of a data breach or non-

342 *Digital Personal Data Protection Act* 2023 (*DPDP Act)*.
343 *DPDP Act*; Bhusan 2024 *International Journal of Advanced Research* 891.
344 Sections 4(1)(a) and 6 of the *DPDP Act*; Sai 2024 *International Journal of Law Management and Huminites* 1055.
345 Sections 4(1)(b) and 7 of the *DPDP Act*; Sai 2024 *International Journal of Law Management and Huminites* 1054.
346 Section 7(a) of the *DPDP Act*; Sharma 2023 *International Journal of Law Management and Humanities* 1845.
347 Section 8(5) of the *DPDP Act*; Sharma 2023 *International Journal of Law Management and Humanities* 1849.
348 Sections 8(10) and 13 of the *DPDP Act*; Seetharamu et al 2024 *International Journal of Scientific Research in Science, Engineering and Technology* 66 and 67.
349 Sections 18(1)(2), and 27 of the *DPDP Act;* Sharma *International Journal of Law Management & Humanities* 1842.
350 Section 10(1) of the *DPDP Act*; Sai 2024 *International Journal of Law Management and Huminites* 1057; The criteria for whether or not these suppliers are based in India is based, *inter alia,* on the amount of sensitive/special personal information the supplier processes and the risks to the privacy rights of consumers.
351 Sections 10(1)(a)(2)(ii) and 27 of the *DPDP Act*; Bhusan 2024 *International Journal of Advanced Research* 891 and 896; Greenleaf 2023 *Privacy Laws & Business International Report* 8.
352 Section 8(7)(a) of the *DPDP Act*; Bhusan 2024 *International Journal of Advanced Research* 892.

compliance with the *DPDP Act* the DPB can institute any remedial measures it deems fit to remedy the adverse effects of a data breach.[353] The DPB can also institute a fine against suppliers who are not in compliance with the provisions of the *DPDP Act.*[354] If a supplier does not incorporate reasonable security safeguards they may be fined up to ₹250 million.[355] A fine of up to ₹200 million may be imposed on a supplier who does not notify the board of a data breach.[356] A fine of ₹150 million may be given to a supplier who has not taken the extra steps required of them due to the type of personal information they process and the scale in which they process personal information.[357] Suppliers who breach section 15 of the *DPDP Act* may be fined an amount of up to ₹10 thousand.[358] A supplier may be fined a maximum amount of ₹50 million for breaching any other provision in the *DPDP Act.*[359] The *DPDP Act* mandates that suppliers processing large volumes of sensitive personal information[360] must appoint a Data Protection Officer based in India. [361] These Data Protection Officers would be responsible for ensuring that suppliers are compliant with the provisions of the *DPDP Act.*[362] Thus, it can be seen that the *DPDP's* approach to imposing fines is based on the specific contravention that is committed which results in a more structured approach to allocating fines. And the requirement for certain suppliers to have local Data Protection Officers ensures that there is a local point of accountability to oversee compliance and address any privacy-related issues efficiently.

The adoption of the *DPDP Act* was essential for protecting consumer privacy rights in India.[363] The structured approach to administering specific fines for specific offences[364]

---

353 Section 27(1)(a) of the *DPDP Act*; Saurabh 2024 *International Journal in Changing World* 87 and 88.

354 Section 33(1) of the *DPDP Act;* Chandramohan et al 2023 *The Lancet Regional Health* 12.

355 Schedule 1 of the *DPDPD Act;* Bhusan 2024 *International Journal of Advanced Research* 900.

356 Schedule 2 of the *DPDP Act.*

357 Schedule 4 and section 10 of the *DPDP Act.*

358 Schedule 5 of the *DPDP Act.*

359 Schedule 7 of the *DPDP Act.*

360 Section 3 of the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules* 2011; Duraiswami *Journal of Cyber Warfare* 171 and 172; Section 26 of the *POPIA*; In terms of India's privacy framework sensitive personal information, includes relevant sexual information, medical record, financial information, and physical and mental health condition. The South African equivalent of this in terms of the *POPIA* would be the term special personal information.

361 Section 10(1)(a)(2)(ii) of the *DPDP Act;* Greenleaf 2023 *Privacy Laws & Business International Report* 8.

362 Section 10(2)(a)(iii)(iv) of the *DPDP Act*; Sharma 2023 *Iinternational Journal of Law Management & Humanities* 1844.

363 Preamble to the *DPDP* Act; Saurabh 2024 *International Journal of Law in Changing World* 77.

364 See para 4.3.1.

and the requirement for certain suppliers to have local Data Protection Officers[365] are strengths that can be adopted in South Africa's consumer privacy framework. These strengths will be further discussed and analysed below.

4.3.2 Strengths of India's Privacy Framework

From the discussion of the overview of India's regulatory privacy framework, two key strengths could be identified. These are the fine amounts enshrined in the *DPDP Act,* and the localisation of the Data Protection Officer. These strengths are comparatively analysed and discussed below.

4.3.2.1 Specific Fine Amounts for Specific Offences and Comparatively High Fine Amounts

The structured approach to allocating specific maximum fine amounts to specific offences[366] and the comparatively high fine amounts enshrined in the *DPDP Act*[367] is considered a strength in India's consumer privacy framework. The *POPIA's* maximum fine amount of R10 million is a fine amount allocated to all *POPIA*-related offences.[368] The *DPDP Act's* provision for specific maximum fines for specific offences is a strength, as it deters violations by establishing clear consequences for non-compliance while reducing discretion and potentially ensuring consistent enforcement. Additionally, some of the fine amount values in the *DPDP Act*[369] are higher than the R10 million maximum fine amount contained in the *POPIA.*[370] This is a strength because, as discussed in paragraph 4.2.3.1 fines that are more proportionate to a supplier's revenue can act as an effective deterrent against prohibited conduct. Thus, the *DPDP Act's* fine amounts which are more proportionate to a supplier's revenue, could enhance accountability and strengthen the enforcement of privacy rights by effectively discouraging non-compliance. Thus, the *DPDP Act's* structured approach to fines, including fine amounts that are more proportionate to a supplier's revenue,

---

365 See para 4.3.1.
366 Schedule of the *DPDP Act;* Bhusan 2024 *International Journal of Advanced Research* 900.
367 Schedule 1 and 2 of the *DPDP Act*; Bhusan 2024 *International Journal of Advanced Research* 900.
368 Section 109(1)(c) of the *POPIA*; Roos 2023 *THRHR* 24.
369 Schedule of the *DPDP Act*; Bhusan 2024 *International Journal of Advanced Research* 900.
370 Section 109(1)(c) of the *POPIA*; van Eeden and Barnard *Consumer Protection Law in South Africa* 572.

could enhance accountability and strengthen the enforcement of privacy rights by effectively discouraging non-compliance.

4.3.2.2 Localisation of the Data Protection Officer

The *DPDP Act* requires suppliers who process large amounts of sensitive personal information[371] to have a Data Protection Officer[372] who is based in India.[373] Whereas, the *POPIA* makes no mention of requiring suppliers who process large amounts of personal information to have Information Officers present in South Africa.[374] This is a strength because it ensures that suppliers who are either within or outside the borders of India can be easily held directly responsible for any sort of grievance that may occur from contravening the provisions of the *DPDP Act.*[375] By requiring suppliers who process a large amount of sensitive personal information to have Data Protection Officers within the borders of India it ensures that stringent processing requirements with regards to sensitive personal information are upheld and that suppliers are more easily held accountable.

4.4 Conclusion

A comparative analysis of the EU and India's privacy frameworks reveals several strengths present in each framework. The identified strengths found in the EU privacy framework include the fine amounts and the requirement for not-for-profit institutions to institute a claim for damages on behalf of the consumer.[376] Additionally, the other strengths present in the EU consumer privacy framework are the presence of a determinable notification period and AI-specific legislation.[377] These strengths present in the EU consumer privacy framework can provide guidance on what South Africa

---

371 *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules* 2011; Duraiswami *Journal of Cyber Warfare* 171 and 172.

372 Sections 2(l) and 10(2)(a)(iii)(iv) of the *DPDP Act*; Saurabh 2024 *International Journal of Law in Changing World* 89; Suppliers processing large amounts of sensitive personal information must appoint Data Protection Officers who serve as the point of contact for grievance and redress issues under the *DPDP Act.* The South African equivalent of a Data Protection Officer would be the Information Officer enshrined in the *POPIA.*

373 Section 10(1)(a)(2)(ii) of the *DPDP Act;* Greenleaf 2023 *Privacy Laws & Business International Report* 8.

374 Section 55 of the *POPIA*; van Eeden and Barnard *Consumer Protection Law in South Africa* 578.

375 Section 10(2)(a)(iv) of the *DPDP Act;* Saurabh 2024 *International Journal of Law in Changing World* 89; Sai *International Journal of Law Management & Humanities* 1057.

376 See para 4.2.3.2.

377 See paras 4.2.3.3 and 4.2.3.4.

can incorporate into its own privacy framework to better protect consumer privacy in the digital age. The strengths of India's privacy framework which are its structured approach to administering fines for specific offences and the comparatively high fine amounts, and the localisation of the Data Protection Officer also provide for potential remedies for the identified weaknesses present in South Africa's privacy framework.[378]

In the next chapter, the researcher will provide recommendations that can be incorporated into South Africa's privacy framework to provide consumers with a more robust privacy protection framework. The next chapter will also provide a conclusion on whether or not South Africa's privacy framework is good enough to effectively protect the consumers right to privacy in the digital age.

[378] See paras 4.3.2.1 and 4.3.2.2.

CHAPTER FIVE

RECOMMENDATIONS AND CONCLUDING REMARKS

5.1 Introduction

South Africa's current regulatory framework for consumer privacy is not as effective as it could be in efficiently protecting the consumer's right to privacy in the digital age. This is due to challenges affecting the efficiency of the regulatory framework, as discussed in Chapter Three of this study. Such challenges include an administrative fine amount that is too low for online privacy-related infringements,[379] the Information Regulator being unable to award damages directly to an aggrieved consumer,[380] and the lack of Artificial Intelligence (AI)-specific legislation.[381] Other identified challenges in South Africa's consumer privacy framework that hinder its effectiveness are the lack of a determinable notification period in instances of data breaches,[382] not requiring suppliers who process a large amount of special personal information to have information officers situated in South Africa,[383] and the lack of a statutorily mandated opt-in/opt-out registry.[384] These identified weaknesses could be remedied by identifying and applying relevant legislative provisions present in India's and the European Union's (EU) privacy framework.

In this chapter, the author will provide some recommendations to remedy the identified weaknesses in South Africa's regulatory framework for consumer privacy. These recommendations are aimed at enhancing South Africa's regulatory framework for consumer privacy in the digital age. This will then be followed by an overall conclusion for the entire mini-dissertation.

5.2 Recommendations

The researcher submits that, *inter alia,* six recommendations can be applied to South Africa's consumer privacy framework. These six recommendations as discussed

379 See para 3.6.2.
380 See para 3.6.1.
381 See para 3.6.3.
382 See para 3.6.4.
383 See para 3.6.5.
384 See para 3.6.6.

below could align South Africa's consumer privacy framework with global standards. Accordingly, it is recommended that the *POPIA* should be amended to provide for an increase in the administrative fine amount, the *POPIA* should be amended to empower the Information Regulator to make an award for monetary damages to consumers, and AI-specific legislation should be enacted. Additionally, it is recommended that the *POPIA* should be amended to require an explicit 72-hour notification period to consumers, the *POPIA* should be amended to require a mandatory 72-hour notification period for data breaches, and the *POPIA* should be so that international suppliers who process large amounts of special personal information should have information situated in South Africa. Lastly, a legally mandated opt-in/opt-out registry should be established.

5.2.1 The POPIA Should be Amended to Provide for an Increase in the Administrative Fine Amount

The unequal bargaining power between consumers and suppliers has resulted in the adoption of specific pieces of legislation that were aimed at lessening this unequal bargaining position between consumers and suppliers.[385] The South African consumer privacy regulatory framework makes provision for enforcement mechanisms[386] and penalties[387] to ensure that suppliers are upholding the *CPA's* aim of creating a fair and equitable marketplace.[388] One of the penalties in South Africa's privacy regulatory framework to enforce compliance with consumer protection legislation is the fine imposed for non-compliance with section 109(1)(c) of the *POPIA.*[389]

High fine amounts can be effective deterrents against prohibited behaviour if the fine amount is proportional to the supplier's annual turnover.[390] However, the R10 million

---

385 Jacobs et al 2010 *PER/PELJ* 353 and 356; Naudé and Eiselen "Introduction and Overview of the Consumer Protection Act" 13; Hawthorne 2008 *THRHR* 440.

386 Section 69 of the CPA; Section 40(1) of the *POPIA*; Jacobs et al 2010 *PER/PELJ* 307 and 308; Schultz and Freedman 2023 *PER/PELJ* 20.

387 Sections 95(1), 99(1), and 109(1)(c) of the *POPIA*; Swales et al 2022 *South African Journal of Science* 2.

388 Section 3(1)(a) of the *CPA*; Jacobs et al 2010 *PER/PELJ* 304; Reddy and Rampersad 2012 *African Journal of Business Management* 7403 and 7404.

389 Section 109(1)(c) of the *POPIA*; Jones *Penn State Journal of Law and International Affairs* 235.

390 Lund and Sarin 2021 *Texas Law Review* 292; Clinard 1982 *Michigan Law Review* 978; Feess et al 2018 *Journal of Economic Behavior and Organization* 59 and 71; Article 101(3) of the *EU AI Act*.

maximum fine amount contained in section 109(1)(c) of the *POPIA* is too low,[391] especially when compared to the annual turnover of major tech companies.[392] Comparatively, the EU's maximum fine amount of €20 million or up to four per cent of supplier's annual turnover[393] and India's maximum fine amount of ₹250 million is comparably more proportionate to suppliers with a high annual turnover.[394] The author recommends that section 109 of the *POPIA* should be amended to include a fine amount that is more in proportion to a supplier's revenue. This follows that a larger maximum administrative fine amount could serve as a more effective deterrent against suppliers who contravene the *POPIA*.[395] The proposed *POPIA* amendment should align with international standards by increasing the maximum administrative fine amount to 400 million[396] or up to four percent of a supplier's annual turnover. This ensures that fines are more proportionate to large suppliers' annual turnover and thus act as a more effective deterrent.

Additionally, the *POPIA* should be amended to include specific maximum fine amounts allocated for particular *POPIA*-related offences. For example, if a supplier does not implement effective security safeguards, as enshrined in the *POPIA*,[397] they should be fined a maximum of R400 million. Similarly, if a supplier contravenes the *POPIA* by not allowing consumers to delete their personal information,[398] they should be fined up to R250 million.[399] This structured approach to allocating specific fine amounts for specific *POPIA* offences could enhance compliance by providing easily determinable

391 Section109(1)(c) of the *POPIA*; Swales et al 2022 *South African Journal of Science* 2.

392 Doan and Nguyen 2022 *International Journal of Current Science Research and Review* 1092-1094; Vandezande 2019 *International Journal for the Data Protection Officer, and Privacy Counsel* 18; Tambou 2019 *European Data Protection Law Review* 80; De-Yolande et al 2023 *Voice of the Publisher* 335; Lund and Sarin 2021 *Texas Law Review* 291 and 292; For example, Google, Apple, and Meta are tech companies that generate tens of billions of dollars in yearly revenue. A R10 million fine for these large companies is a comparatively low amount compared to their annual revenue, and thus not an effective deterrent.

393 Article 83(5) of the *GDPR*; Vandezande 2019 *International Journal for the Data Protection Officer, and Privacy Counsel* 17.

394 Schedule 1 of the *DPDP Act;* Bhusan 2024 *International Journal of Advanced Research* 900.

395 Section 109 of the *POPIA*; Swales et al 2022 *South African Journal of Science* 2; Clinard 1982 *Michigan Law Review* 978.

396 At the time of writing this chapter, the Euro-to-Rand conversion rate was R19.94 per €1. This R400 million maximum fine amount is largely based on a direct currency conversion of the €20 million amount into Rands.

397 Sections 19-22 of the *POPIA*; van Eeden and Barnard *Consumer Protection Law in South Africa* 576.

398 Section 24(1)(a) of the *POPIA*; Mtuze and Papadopoulos "Privacy and Data Protection" 364.

399 At the time of writing this chapter, the Rupee to Rand conversion rate was R0.22 per ₹1. The R250 million figure was calculated by observing some of the listed fine amounts in the *DPDP Act* and converting them into South African Rands.

consequences for *POPIA* violations. This could also ensure consistent enforcement of the *POPIA's* obligations, and limit ambiguity.

Furthermore, the author recommends that the *POPIA* should be amended to allow the Information Regulator to impose daily fines of up to R2 million on suppliers who do not implement the Information Regulator orders on a timely basis. This is to incentivise suppliers to implement orders made by the Information Regulator in a timely manner.

Therefore, these proposed amendments to the *POPIA* aim to achieve three objectives. Firstly, ensuring fines are proportionate to a supplier's annual turnover. Secondly, allocating specific fine amounts to particular offences to provide clear consequences for violations. Thirdly, imposing daily fines on non-compliant suppliers to promote timely adherence to *POPIA* regulations.

5.2.2 The POPIA Should be Amended to Empower the Information Regulator to Make an Award for Monetary Damages to Consumers

Section 99 of the *POPIA* allows for a consumer to seek damages in the civil courts from suppliers who contravene *POPIA* provisions.[400] This creates an inefficiency in the enforcement of privacy rights. This is because going to court is expensive and time-consuming.[401] A consumer would have to wait for the Information Regulator to conclude its investigation and then the Information Regulator might institute a claim on behalf of a consumer, although it is not legally compelled to.[402]

The author recommends that the Information Regulator should be empowered by the *POPIA* to award damages to consumers who have experienced a data breach. Empowering the Information Regulator to award damages would save consumers significant costs, as they would not need to rely on civil courts to seek compensation for damages.[403] Granting the Information Regulator the authority to award damages

---

400 Section 99(1) of the *POPIA*; Mtuze and Papadopoulos "Privacy and Data Protection" 372.

401 *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* [2021] ZACC 3 para 49 (*AmaBhungane* case); Woker 2010 *Obiter* 231; Peté et al *Civil Procedure: A Practical Guide* 301.

402 Roos 2023 *THRHR* 4; Mantelero 2021 *Computer Law and Security Review* 1; Mtuze and Papadopoulos "Privacy and Data Protection" 330 and 348.

403 *AmaBhungane* case para 49; Woker 2010 *Obiter* 231; Peté et al *Civil Procedure: A Practical Guide* 301.

directly to consumers may negatively impact its current legislative duties,[404] given its currently limited resources and operational capacity.[405] An increase in the Information Regulator's funding should be implemented to ensure it has sufficient institutional resources to carry out this function effectively.[406] Therefore, it is recommended that the *POPIA* should be amended to grant the Information Regulator the authority to award damages to consumers.

Additionally, the author recommends that the *POPIA* should require relevant non-profit institutions to institute a claim for damages on behalf of consumers who have experienced a privacy infringement. Like the Consumer Goods and Services Ombud,[407] these non-profit institutions could be funded by the government and/or the private sector. Therefore, the *POPIA* should be amended to require non-profit institutions to file damage claims in civil court on behalf of aggrieved consumers, reducing the financial burden of litigation on consumers.

Amending the *POPIA* to empower the Information Regulator to award damages and mandating non-profit institutions to file claims on behalf of consumers would go a long way in streamlining the enforcement of consumer privacy rights. This would alleviate the time and financial burden on consumers. These recommended amendments would create a more efficient and accessible consumer enforcement landscape in South Africa.

---

404 Sections 40(1) ,74, 75, 95(1), and 109(1)(c) of the *POPIA*; Bronstein 2022 *PER/PELJ* 4.

405 "Information Regulator Annual Report For the Year Ended 31 March 2023 19 and 47" available at https://inforegulator.org.za/wp-content/uploads/2020/07/Information-Regulator-Annual-Report-2023-Compressed.pdf; "Annual Report for 2023/24 Financial Year for the Information Regulator 89 and 91" available at https://inforegulator.org.za/wp-content/uploads/2020/07/Information-Regulator-Annual-Report-2023_25_Approved-by-Members_Final90.pdf.

406 See "Information Regulator Annual Report For the Year Ended 31 March 2023 19 and 47" available at https://inforegulator.org.za/wp-content/uploads/2020/07/Information-Regulator-Annual-Report-2023-Compressed.pdf; "Annual Report for 2023/24 Financial Year for the Information Regulator 89 and 91" available at https://inforegulator.org.za/wp-content/uploads/2020/07/Information-Regulator-Annual-Report-2023_25_Approved-by-Members_Final90.pdf.

407 *Consumer Goods and Services Ombud NPC v Voltex (Pty) Ltd [2021] ZAGPPHC* 309 paras 8,11, and 72; Du Plessis 2022 *Stell LR* 78.

5.2.3 AI-Specific Legislation Should be Enacted

The ubiquity of AI in everyday life has necessitated the need for AI-specific legislation that can protect consumer privacy rights. AI has many benefits for consumers. One of the relevant benefits of AI is that it can personalise service recommendations based on consumer's personal information.[408] Another benefit of AI is that the use of AI has been shown to improve the overall customer experience for consumers.[409] However, AI can pose privacy risks to South African consumers.[410] An immediate and effective regulatory response to AI may increase the potential benefits AI might have in South Africa.[411] Additionally, an immediate and effective AI regulatory response may lessen the privacy concerns associated with AI.

To maximise the benefits of AI while minimising its negative privacy impacts, the author recommends that the government promptly implement a comprehensive AI regulatory and enforcement framework. International institutions[412] and the South African government have acknowledged the key role AI can play in the improvement of social issues in South Africa.[413] In light of South Africa's 2024 AI policy framework document the researcher suggests that South Africa's proposed AI legislation is formulated in such a way that explicit consumer privacy protections are provided. And that South Africa's proposed AI legislative framework cultivates a fair and equitable digital consumer environment, by, *inter alia,* protecting the right to privacy. The *EU AI Act's* approach to outright banning AI systems that pose a significant risk to fundamental human rights[414] is a regulatory feature that must form part of South Africa's proposed

---

408 Hariguna and Ruangkanjanases 2024 *Data Science and Management* 156; Patras and Theodoridis *Advances in Artificial Intelligence-based Technologies* 155.

409 Bilal et al 2024 *Journal of Retailing and Consumer Services* 1 and 4; Singh and Singh 2024 *Cogent Business and Management* 1 and 9.

410 Section 23-25 of the *POPIA*; *National Media Ltd v Jooste 1996 (3) SA 262 (SCA)* paras 11, and 13-18; Hu and *Min International Journal of Hospitality Management* 2; Saheb 2023 *AI and Ethics* 369,374; Fontes 2022 et al *Technology in Society* 2 and 3; Eliot and Soifer 2022 *Frontiers in Artificial Intelligence* 1; Bartneck *An Introduction to Ethics in Robotics and AI* 2 and 24.

411 "South Africa National Artificial Intelligence Policy Framework 1 and 3" available at https://www.dcdt.gov.za/sa-national-ai-policy-framework/file/338-sa-national-ai-policy-framework.html; Trabelsi 2024 *Journal of Electronic Business and Digital Economics* 152.

412 "Recommendation on the Ethics of Artificial Intelligence 2 and 6" available at https://unesdoc.unesco.org/ark:/48223/pf0000381137; van Norren 2022 *Journal of Information, Communication, and Ethics in Society* 112,123, and 125.

413 "South Africa National Artificial Intelligence Policy Framework 1" available at https://www.dcdt.gov.za/sa-national-ai-policy-framework/file/338-sa-national-ai-policy-framework.html; Trabelsi 2024 *Journal of Electronic Business and Digital Economics* 152.

414 Articles 5(1-5) of the *EU AI Act*; Aboy et al 2024 *NPJ Digital Medicine* 3.

AI regulatory framework as it would be in line with the constitutional values of human rights and dignity.[415] Additionally, AI-specific legislation should ensure that when regulating and protecting consumer privacy, it implements principles of transparency, fairness, and accountability to safeguard privacy rights. The Information Regulator should be the institution that continues to govern/enforce AI-related matters.[416] As a result of this, an increase in the Information Regulator's funding should occur. This is to ensure that the Information Regulator has operational capacity[417] to deal with the increased privacy-related risks that AI poses.[418] Increasing the Information Regulators funding, rather than creating a separate AI-specific institution, would streamline enforcement and prevent consumers from being sent from pillar to post.[419] Thus, it is recommended that South Africa enacts AI-specific legislation and increases the Information Regulator's funding. These proposed measures should also consider South Africa's socio-economic setting to maximise the potential benefits of AI and minimise its drawbacks.

5.2.4 The POPIA Should Be Amended to Provide for an Explicit 72-Hour Notification Period for Data Breaches

The instantaneous nature of the digital world[420] means that swift action must be taken in instances of data breaches. This is due to the negative consequences[421] that may quickly occur if consumers' personal information is accessed by unauthorised persons

---

415 *S v Makwanyane and Another* 1995 (3) SA 391 para 329; *Bernstein and Others v Bester NO and Others* para 77; Currie and de Waal *Bill of Rights Handbook* 6th edition 36, 250, and 251; Florida 2016 *Philosophy and Technology* 307-309.

416 Long title, preamble, sections 4(1),39, and 71 of the *POPIA*; van Eeden and Barnard *Consumer Protection Law in South Africa* 568.

417 "Information Regulator Annual Report For the Year Ended 31 March 2023 19 and 47" available at https://inforegulator.org.za/wp-content/uploads/2020/07/Information-Regulator-Annual-Report-2023-Compressed.pdf; "Annual Report for 2023/24 Financial Year for the Information Regulator 89 and 91" available at https://inforegulator.org.za/wp-content/uploads/2020/07/Information-Regulator-Annual-Report-2023_25_Approved-by-Members_Final90.pdf.

418 Section 23-25 of the *POPIA*; *National Media Ltd v Jooste 1996 (3) SA 262 (SCA)* paras 11, and 13- 18; Hu and *Min International Journal of Hospitality Management* 2; Saheb 2023 *AI and Ethics* 369 and 374; Fontes 2022 et al *Technology in Society* 2 and 3; Eliot and Soifer 2022 *Frontiers in Artificial Intelligence* 1; Bartneck *An Introduction to Ethics in Robotics and AI* 2 and 24.

419 See *MFC (a division of Nedbank Ltd) v Botha* (6981/13) [2013] ZAWCHC 107 para 9; Otto et al 2014 *SA Merc LJ* 247.

420 Jones 2021 *Penn State Journal of Law and International Affairs* 220 and 221; Kozyreva et al 2020 *Psychological Science in the Public Interest* 105 and 108.

421 Bargavi et al 2022 *International Journal of Data Informatics and Computing* 53; Mausch et al 2022 *Computers and Security* 9.

or entities. These negative consequences can include, identity theft,[422] unsolicited direct communication,[423] monetary theft,[424] and fraud.[425] This results in consumers needing to be timeously informed about data breaches involving their personal information so that they can take steps to mitigate the negative consequences of data breaches. South Africa's privacy framework does not currently have a determinable notification period that suppliers must adhere to when notifying consumers that their personal information has been unlawfully accessed. Currently, the *POPIA* stipulates that suppliers must notify consumers as soon as reasonably possible about data breaches that affect their personal information.[426]

The flexible nature of the concept of reasonableness leaves the timeframe for reporting a data breach to the Information Regulator and the consumer at the supplier's discretion.[427] It is submitted that the *POPIA* should be amended to explicitly state that 72 hours is the maximum period that suppliers should have to notify the Information Regulator and the consumer of a data breach. This 72-hour notification period would align with international best practice, the *GDPR*.[428] This is to ensure that consumers can timeously safeguard themselves against the negative consequences that they might experience from the data breach.

Establishing an explicit notification period of 72 hours in the *POPIA* would provide greater consistency and certainty in responding to data breaches. This amendment would improve consumer privacy protection by ensuring timely notification, which could allow consumers to take prompt action to mitigate potential harm.

---

422 Strzeleck and Rizun 2022 *Sustainable E-commerce* 2 and 3; Bargavi et al 2022 *International Journal of Data Informatics and Intelligent Computing* 53 and 55.

423 Labreque et al 2021 *Journal of Business Research* 559; Strzeleck and Rizun 2022 *Sustainable E-commerce* 5.

424 Labreque et al 2021 *Journal of Business Research* 560; Wang et al 2019 *Issues in Information Systems* 162.

425 Makridis 2021 *Journal of Cybersecurity* 2; Ho et al *Sage Journals* 1 and 3; Labreque 2021 *Journal of Business Research* 559; Wang et al 2019 *Issues in Information Systems* 162.

426 Section 22(2) of the *POPIA*; Roos 2023 *THRHR* 20.

427 Section 22(2) of the *POPIA*; Bronstein 2022 *PER/PELJ* 14.

428 Article 33(1) of the *GDPR*; Roos 2023 *THRHR* 4; Mtuze and Papadopoulos “Privacy and Data Protection” 330 and 348; De-Yolande 2023 *Voice of the Publisher* 356.

5.2.5 International Suppliers who Process Large Amounts of Special Personal Information Should Have Information Officers Situated in South Africa

Special personal information potentially carries with it a greater risk to the consumer if it is unlawfully processed.[429] This is due to the increased negative consequences[430] that may occur if said special personal information is unlawfully accessed. Information Officers are entrusted with ensuring compliance with the *POPIA* provisions. In instances of data breaches, collaboration between South Africa's Information Regulator and a foreign supplier's Information Officer may be difficult. Currently, no legislation in South Africa's privacy framework requires suppliers who process a large amount of South African consumers' special personal information to have Information Officers who are situated in South Africa.

It is recommended that the *POPIA* be amended to require that internationally-based suppliers who process a large amount of special personal information must have Information Officers situated in South Africa. This could ensure that global companies headquartered abroad have a local point of accountability, making it easier to address *POPIA*-related inquiries or issues and ensure greater compliance with South Africa's privacy framework. Additionally, this proposed amendment may reduce the risk of South African consumers' sensitive personal information being mishandled in countries with inadequate privacy enforcement frameworks.[431]

Requiring suppliers who process large amounts of special personal information to have Information Officers in South Africa could enhance accountability and streamline compliance with South Africa's privacy laws. This amendment might ensure stronger privacy protections for South African consumers by providing a local point of contact and reducing risks associated with weak privacy enforcement frameworks in foreign countries.

---

429 Labreque et al 2021 *Journal of Business Research* 563; Quinn and Malgieri 2021 *German Law Journal* 1583.

430 Mosesson et al 2022 *Plos One* 1 and 2; *Belen-Saglam* et al 2022 *Frontiers in Computer Science* 2,3, and 8; The heightened risks consumers face from data breaches or unlawful access to their sensitive information are particularly evident when suppliers hold potentially incriminating or life altering special personal information.

431 Pelteret and Ophoff 2016 *Informing Science: The International Journal of an Emerging Transdiscipline* 277,281, and 282; Ademuyiwa and Adeniran 2020 *Centre for International Governance Innovation* 4-6; Chatsuwan et al *Heliyon* 2023 1 and 24.

5.2.6 The Establishment of a Harmonised Opt-Out/Opt-In Registry

The proposed *CPA* amendments to establish an opt-out registry is a step in the right direction, and thus the researcher recommends that legislative intervention takes place in order to establish a national opt-out registry. The proposed *CPA* amendments puts the operation of the registry under the custodianship of the National Consumer Commission.[432] The researcher submits that the running of the opt-out registry should fall under the Information Regulator's jurisdiction. Multiplicity of institutions in South Africa's consumer framework can result in consumers being sent from pillar to post,[433] which can negatively impact the efficacy of the enforcement of consumer privacy rights. To avoid multiplicity of institutions that deal with the same legal complaints/issues the proposed *CPA* amendment should bring the operation of the proposed opt-out/opt-in registry into the Information Regulator's jurisdiction. This could result in either an amendment to the *CPA* or an amendment to section 69 of the *POPIA*.[434] This registry could allow consumers to choose whether or not they wish to opt-in to receiving direct marketeering material. Or alternatively, consumers could provide their details to the national registry to opt-out of receiving direct marketing material. The efficacy of an established opt-in registry in protecting consumer privacy rights can be seen in Ireland's opt-out registry regime.[435] An increase in the Information Regulator's funding to ensure it has the capacity to set up an opt-in registry and the capacity to enforce relevant *POPIA* provisions against direct marketers would be needed. Legislators should harmonise both opt-in and opt-out approaches enshrined in the *POPIA*[436] and the *CPA*[437] in order to provide consumers with the most amount of privacy protections. Thus, aligning the *CPA's* proposed opt-out registry with the *POPIA's* opt-in framework under the authority of the Information Regulator would

---

432 Schedule (3)(d)(10) in GN R2798 in GG 51436 of 28 October 2024.

433 See *MFC (a division of Nedbank Ltd) v Botha* (6981/13) [2013] ZAWCHC 107 para 9; Otto et al 2014 *SA Merc LJ* 247.

434 Section 69 of the *POPIA*; Zenda et al 2020 *South African Computer Journal* 114.

435 Regulation 1,13, and 14 of the *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations* 2011; "Annual Report of the Data Protection Commission 2007 9-11, 14, 20, 26, and 48" available at https://www.dataprotection.ie/sites/default/files/uploads/2018-12/AR2007En.pdf; McBride 2012 *BMC Medical Research Methodology* 4; Ireland's opt-out regime provides consumers with the opportunity of opting out of receiving direct marketing materials on a statutorily mandated opt-out registry.

436 Section 69(1) of the *POPIA*; Zenda et al 2020 *South African Computer Journal* 114.

437 Section 11(1)(2) of the *CPA*; Schedule of 3 in GN R2798 in GG 51436 of 28 October 2024; Eiselen et al "Section 11" 11-1.

create a more cohesive, efficient, and enforceable consumer privacy regime. Additionally, the establishment of such a registry would significantly enhance privacy protections under the *CPA* by providing consumers with a centralised, accessible mechanism to manage their direct marketing preferences.

5.3 Concluding Remarks

The explosive rise of e-commerce[438] and the emerging ubiquity of AI[439] has necessitated the need for a robust and efficient regulatory framework for consumer privacy in South Africa. The previous common law-dominated privacy framework, which still forms part of South Africa's privacy framework, was inadequate in key areas which resulted in the need for a legislative framework to supplement the protection of consumer privacy in South Africa. The promulgation of the *Constitution*, the *ECTA*, the *CPA*, and the *POPIA* have provided some reprieve to the deficiencies present in the common law privacy framework. However, South Africa's legislative privacy framework is not without its issues.

To address the six identified weaknesses discussed throughout this study, several recommendations were made. Firstly, it was recommended that the *POPIA* should be amended to ensure that the administrative fine amount contained in the *POPIA* is increased to ensure that administrative fine amounts are proportionate to larger suppliers' annual turnover. Secondly, it was recommended that the *POPIA* should be amended to empower the Information Regulator with the ability to award monetary damages to aggrieved consumers. Thirdly, it was recommended that the government should urgently promulgate AI-specific legislation. Fourthly, it is recommended that the *POPIA* be amended to stipulate that suppliers must notify consumers and the Information Regulator within 72 hours of becoming aware of a data breach. Fifthly, the *POPIA* should be amended so that suppliers who process a large amount of South African consumers' special personal information must have Information Officers who are situated in South Africa. Sixthly, it was recommended that there be a statutorily established opt-in/opt-out registry. These recommendations should provide for a more

438 Gupta et al 2023 *Sustainable Operations and Computers* 200 and 207; Sharma and Mishra 2023 *Journal of Namibian Studies History Politics Culture* 1838.

439 Butson and Spronken-Smith 2024 *Higher Education Research and Development* 564; Bilal et al 2024 *Journal of Retailing and Consumer Services* 1.

robust and efficient privacy regulatory and enforcement privacy framework for South African consumers.

Bibliography

Literature

Abdulrauf et al 2024 *SAJBL*

Abdulrauf L et al "Clarifying the Legal Requirement for Cross-Border Sharing of Health Data in POPIA: Recommendations on the Draft Code of Conduct for Research" 2024 *SAJBL* 44-48

Aboy et al 2024 *NPJ Digital Medicine*

Aboy et al "Navigating the EU AI Act: implications for regulated digital medical products" 2024 *NPJ Digital Medicine* 1-5

Adams et al 2021 *South African Journal of Science*

Adams R et al "POPIA Code of Conduct for Research" *South African Journal of Science* 2021 1-12

Ademuyiwa and Adreniran 2020 *Centre for International Governance Innovation*

Ademuyiwa I and Adreniran A "Assessing Data Protection and Privacy in Africa" 2020 *Centre for International Governance Innovation* 4-6

Ahamad et al 2023 *Humanities and Social Sciences Communications*

Ahamad FS et al "Impact of Artificial Intelligence on Human Loss in Decision Making, Laziness and Safety in Education" 2023 *Humanities and Social Sciences Communications* 1-11

Ahmed 2019 *PER/PELJ*

Ahmed R "The Influence of Reasonableness on the Element of Conduct in Delictual or Tort-Liability-Comparative Conclusions" 2019 *PER/PELJ* 1-25

Asimow 1996 *American Journal of Comparative Law*

Asimow M "Administrative Law under South Africa's Interim Constitution" 1996 *American Journal of Comparative Law* 393-420

Aspers 2019 *Qualitative Sociology*

Aspers O and Corte Ugo "What is Qualitative in Qualitative Research" 2019 *Qualitative Sociology* 139-160

Barnard 2021 *International Journal on Consumer Practice*

Barnard J "An Overview of the Consumer Safety and Product Liability Regime in South Africa" 2021 *International Journal on Consumer Practice* 26-51

Bartneck C et al *An Introduction to Ethics in Robotics and AI*

Bartneck C et al *An Introduction to Ethics in Robotics and AI (SpringerBriefs in Research and Innovation Governance* 2021)

Basimanyane 2022 *African journal of international and Comparative Law*

Basimanyane D "The Regulatory Dilemma on Mass Communications Surveillance and the Digital Right to Privacy in Africa: The Case of South Africa" 2022 *African journal of international and Comparative Law* 361-382

Bauling and Nagtegaal 2015 *De Jure*

Bauling A and Nagtegaal A "Bread as Dignity: The Constitution and the Consumer Protection Act 68 of 2008" 2015 *De Jure* 149-171

Belen-Saglam 2022 *Frontiers in Computer Science*

Belen-Saglam R et al "An Investigation Into the Sensitivity of Personal Information and Implications for Disclosure: A UK Perspective" 2022 *Frontiers in Computer Science* 1-20

Bhusan 2024 *International Journal of Advanced Research*

Bhusan V "Empowering Individuals: A Deep Dive Into the Digital Personal Data Protection Act, 2023 " 2024 *International Journal of Advanced Research* 891-902

Boerman and Smit 2022 *International Journal of Advertising*

Boerman SC and Smit EG "Advertising and Privacy: An Overview of Past Research and a Research Agenda" 2022 *International Journal of Advertising* 60-68

Borgesius 2023 *Scripted*

Borgesius FZ et al "The GDPR's Rules on Data Breaches: Analysing Their Rationales and Effects" 2023 *Scripted* 352-382

Botha et al 2019 *De Serie Legenda Developments in Specific Contracts and Consumer Protection Law Vol II*

Botha MM et al *De Serie Legenda Developments in Specific Contracts and Consumer Protection Law Vol II* (LexisNexis South Africa 2019)

Bottis and Bouchagiar 2018 *Open Journal of Philosophy*

Bottis M and Bouchagiar G "Personal Data v. Big Data: Challenges of Commodification of Personal Data" 2018 *Open Journal of Philosophy* 206-215

Boura 2024 *Athens Journal of Law*

Boura M “The Digital Regulatory Framework through EU AI Act: The Regulatory Sandboxes' Approach” 2024 *Athens Journal of Law* 385-398

Breitbarth 2018 *European Data Protection Law Review*

Breitbarth P "Netherlands: The GDPR Implementation Act" 2018 *European Data Protection Law Review* 360-365

Bronstein 2022 *PER/PELJ*

Bronstein V “Prioritising Command-and-Control Over Collaborative Governance: The Role of the Information Regulator Under the *Protection of Personal Information Act*” 2022 *PER/PELJ* 2-31

Büchi 2017 et al *Information, Communication & Society*

Büchi m et al “Caring is Not Enough: The Importance of Internet Skills for Online Privacy Protection” 2017 *Information, Communication & Society* 1261-1278

Butson and Spronken-Smith 2024 *Higher Education Research and Development*

Butson R and Spronken-Smith R “AI and Its Implications for Research in Higher Education: A Critical Dialogue” 2024 *Higher Education Research and Development* 563-577

Chandramohan et al 2023 *The Lancet Regional Health*

Chandramohan A et al ” Teleradiology and Technology Innovations in Radiology: Status in India and its Role in Increasing Access to primary health Care” 2023 *The Lancet Regional Health* 1-13

Chatsuwan et al 2023 *Heliyon*

Chatsuwan P et al “Personal Data Protection Compliance Assessment: A Privacy Policy Scoring Approach and Empirical Evidence from Thailand's SMEs” 2023 *Heliyon* 1-25

Chaturvedi et al 2020 *Young Consumers*

Chaturvedi P et al “Investigating the Determinants of Behavioural Intentions of Generation Z for Recycled Clothing: An Evidence from a Developing Economy” 2020 403-412

Clinard 1982 *Michigan Law Review*

Clinard MB “Review of Corporate Crime” 1982 *Michigan Law Review* 978-980

Costa and Rodrigues 2024 *Review of Managerial Science*

Costa P and Rodrigues H “The Ever-Changing Business of E-Commerce-Net Benefits while Designing a New Platform for Small Companies” 2024 *Review of Managerial Science* 2507-2545

Craig 2013 *Current Legal Problems*

Craig P "*The Nature of Reasonableness Review"* 2013 *Current Legal Problems* 131-167

Currie and de Waal *Bill of Rights Handbook*

Currie I and de Waal J *Bill of Rights Handbook* 6th (Juta Cape Town 2013)

Dancaster and Dancaster 1995 *SAMJ*

Dancaster JT and Dancaster LA "Confidentiality Concerning HIV/Aids Status-the Implications of the Appeal Court Decision" 1995 *SAMJ* 141-145

de Hart and Czerniawski 2016 *International Data Privacy Law*

de Hart P and Czerniawski M "Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context" 2016 *International Data Privacy Law* 230-246

de Waal 2022 *Current Allergy and Clinical Immunology*

de Waal PJ "The Protection of Personal Information Act (POPIA) and the Promotion of Access to Information Act (PAIA): is it Time to Take Note?" 2022 *Current Allergy and Clinical Immunology* 232-236

De-Yolande et al 2023 *Voice of the Publisher*

De-Yolande D et al "Breach Notification in the General Data Protection Regulation" 2023 *Voice of the Publisher* 334-347

Dhamija 2020 *South African Journal of Economics*

Dhamija P " Economic Development and South Africa: 25 Years Analysis (1994 To 2019) " 2020 *South African Journal of Economics* 298-317

Doan and Nguyen 2022 *International Journal of Current Science and Research*

Doan TNT and Nguyen HH "Value Creation and Value Capture: Analysis of Apple Company" 2022 *International Journal of Current Science and Research* 1089-1095

Du Plessis 2007 *Journal for Juridical Science*

Du Plessis "Access to Justice Outside the Conventional Mould: Creating a Model for Alternative Clinical Legal Training" 2007 *Journal for Juridical Science* 44-63

Du Plessis 2018 *SA Merc LJ*

Du Plessis "Access to Redress for Consumers: A Tale of the Effect of a Notice of Non-Referral by the National Consumer Commission" 2018 *SA Merc LJ* 330-337

Du Preez 2009 *Journal of South African Law*

Du Preez ML "The Consumer Protection Bill: A Few Preliminary Comments" 2009 *Journal of South African Law* 58-85

Duraiswami 2017 *Journal of Law & Cyber Warfare*

Duraiswami DR “Privacy and Data Protection in India" 2017 *Journal of Law & Cyber Warfare* 58-85

Dwivedi et al 2023 *Technological Forecasting and Social Change*

Dwivedi YK et al “Evolution of Artificial Intelligence Research in Technological Forecasting and Social Change: Research Topics, Trends, and Future Directions” 2023 *Technological Forecasting and Social Change* 1-13

Eiselen 2021 *TSAR*

Eiselen S "Digitisation and Consumer Law in South Africa and Africa" 2021 *TSAR* 436-455

Eiselen Section 11”

Eiselen S “Section 11” in Naudé T and Eiselen s (eds) *Commentary in the Consumer Protection Act* (Juta Claremont 2014) ch 11

Elliot D and Soifer E 2022 *Frontier in Artificial Intelligence*

Elliot D and Soifer E “AI Technologies, Privacy, and Security” 2022 *Frontier in Artificial intelligence* 1-8

Esteve 2017 *International Data Privacy Law*

Esteve A “The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA” 2017 *International Data Privacy Law* 36-47

Feess et al 2021 *Journal of Economic Behavior and Organization*

Feess E et al “The impact of Fine Size and the Uncertainty on Punishment and Deterrence: Theory and Evidence from the Laboratory” 2021 *Journal of Economic Behavior and Organization* 58-73

Floridi 2016 *Philosophy and Technology*

Floridi L “On Human Dignity as a Foundation for the Right to Privacy” 2016 *Philosophy and Technology* 307-312

Fontes et al 2022 *Technology in Society*

Fontes C et al “AI-Powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them” 2022 *Technology in Society* 1-10

Frederick and Davids 1995 *Journal of South African Law*

Frederick IN and Davids LC "The Privacy of Wife Abuse" 1995 *Journal of South African Law* 471-492

Fritz 2021 *Constitutional Review*

Fritz C “South African Taxpayers’ Right to Privacy in Cross-Border Exchange of Tax Information” 2021 *Constitutional Court Review* 1-22

Gravett 2020 *Southern African Public Law Journal*

Gravett W “The Dark Side of Artificial Intelligence: Challenges for the Legal System” 2020 *Southern African Public Law Journal* 1-24

Greenleaf 2023 *Privacy Laws & Business International Report*

Greenleaf G “India’s 2023 Data Privacy Act: Business/government Friendly, Consumer Hostile” 2023 *Privacy Laws & Business International Report* 3-12

Gilbert 2024 *Digital Medicine*

Gilbert S “The EU Passes the AI Act and its Implications for Digital Medicine are Unclear” 2024 *Digital Medicine* 1-3

Guadamuz 2024 *The Journal of World Intellectual Property*

Guadamuz A “The EU's Artificial Intelligence Act and copyright” 2024 *The Journal of World Intellectual Property* 1-6

Hariguna and Ruangkanjanases 2024 *Data Science Management*

Hariguna T and Ruangkanjanases A “Assessing the Impact of Artificial Intelligence on Customer Performance: A Quantitative Study Using Partial Least Squares Methodology” 2024 *Data Science Management* 155-163

Henson 2024 *Missouri Law Review*

Henson R “Bridging the Divide: Does the EU's AI Act Offer Code for Regulating Emergent Technologies in America?” 2024 *Missouri Law Review* 847-870

Heyns and Kilbourn 2022 *Journal of Transport and Supply Chain Management*

Heyns GJ and Kilbourn PJ "Online Shopping Behaviour and Service Quality Perceptions of Young People in South Africa: A COVID-19 Perspective" 2022 *Journal of Transport and Supply Chain Management* 1-13

Hoofnagle et al 2019 *Information Technology & Communications Law*

Hoofnagle CJ et al “The European Union General Data Protection Regulation: What It Is and What It Means” 2019 *Information Technology & Communications Law* 65-98

Hu 2020 *Big Data & Society*

Hu M “Cambridge Analytica’s Black Box” 2020 *Big Data & Society* 1-4

Hu and Min 2023 *International Journal of Hospitality Management*

Hu Y and Min HK "The Dark Side of Artificial Intelligence in Service: The "Watching-Eye" Effect and Privacy Concerns" 2023 *International Journal of Hospitality Management* 1-9

Hungwe and Munoriyarwa 2024 *Statue Law Review*

Hungwe B and Munoriyarwa A "An Analysis of the Legislative Protection for Journalists and Lawyers Under Zimbabwe's Interception of Communications Act" 2024 *Statue Law Review* 1-18

Issaoui et al 2023 *Future Business Journal*

Issaoui A et "Exploring the General Data Protection Regulation (GDPR) Compliance in Cloud Services: Insights from Swedish Public Organizationso n Privacy Compliance" 2023 *Future Business Journal* 1-13

Data Protection Law in Germany, the United States, and China. In: Data Privacy and Crowdsourcing

Hornuf L et al *Data Protection Law in Germany, the United States, and China. In: Data Privacy and Crowdsourcing* (Springer Switzerland 2023)

Jacobs et al 2023 *PER/PELJ*

Jacobs W et al "Fundamental Consumer Rights Under the Consumer Protection Act 68 Of 2008: A Critical Overview and Analysis" 2023 *PER/PELJ* 302-398

Jain 2019 *Nirma University Law Journal*

Jain S "Artificial Intelligence: A Threat to Privacy?" 2019 *Nirma University Law Journal* 21-36

Jáñez-Martino et al 2023 *Artificial Intelligence Review*

Jáñez-Martino F et al "A Review of Spam Email Detection: Analysis of Spammer Strategies and the Dataset Shift Problem" 2023 *Artificial Intelligence Review* 1145–1173

Jephson 2014 Constitutional Court Review

Jephson G "A False Start in the Development of Class Action Law: Mukaddam and Others v Pioneer Food (Pty) Ltd and Others" Constitutional Court Review 286- 299

Jones 2021 *Penn State Journal of Law and International Affairs*

Jones B “Is POPIA Bad Business for South Africa? Comparing the GDPR to POPIA and Analyzing POPIA's Impact on Businesses in South Africa” 2021 *Penn State Journal of Law and International Affairs* 217-248

Kędzior 2021 *ERA Forum* 21-36

Kędzior M “The Right to Data Protection and the COVID-19 Pandemic: the European Approach” 2021 *ERA Forum* 533–543

Kandeh et al 2018 *South African Journal of Information Management*

Kandeh AT et al “Enforcement of the *Protection of Personal Information (POPI) Act*: Perspective of Data Management Professionals” 2018 *South African Journal of Information Management* 1-9

Klar 2020 *Hastings Science and Technology Law Journal*

Klar H “Binding Effect of the European General Data Protection Regulation (*GDPR*)” 2020 *Hastings Science and Technology Law Journal* 101-154.

Kozyreva 2020 *Psychological Science in the Public Interest*

Kozyreva A et al 2020 “Citizens Versus the Internet: Confronting Digital Challenges With Cognitive Tools” *Psychological Science in the Public Interest* 103-156

Kraus et al 2021 *IJEBR*

Kraus S et al “Facebook and the Creation of the Metaverse: Radical Business Model Innovation or Incremental Transformation?” 2021 *IJEBR* 52-77

Kurz et al 2014 *Journal of Experimental Social Psychology*

Kurz T et al 2014 “A Fine Is a More Effective Financial Deterrent When Framed Retributively and Extracted Publicly” *Journal of Experimental Social Psychology* 170-177

Laux et al 2024 *Regulation & Governance*

Laux J et al “Trustworthy Artificial Intelligence and the European Union *AI Act:* On the Conflation of Trustworthiness and Acceptability of Risk” 2024 *Regulation & Governance* 3-32

Levallois-Barth C 2012 *International Data Privacy Law*

Levallois-Barth C “Bluespam and the French National Commission on data Protection (CNIL)” 2012 *International Data Privacy Law* 19-25

Liu 2024 *Journal of Education, Humanities and Social*

Liu Z “A Financial Analysis of Apple based on its External and Internal Environment” 2024 *Journal of Education, Humanities and Social Sciences* 97-104

Luisi 2022 *E-International Relations*

Luisi M “GDPR as a Global Standards? Brussels' Instrument of Policy Diffusion” 2022 *E-International Relations* 1-12

Lund and Sarin 2021 *Texas Law Review*

Lund DS and Sarin N “Corporate Crimes and Punishment: An Empirical Study” 2021 *Texas Law Review* 284-352

Lochner 2022 et al *Journal of Psychiatric Research*

Lochner C et al “The Covid-19 Pandemic and Problematic Usage of the Internet: Findings from a Diverse Adult Sample in South Africa” 2022 *Journal of Psychiatric Research* 229-235

Lockaht 2021 *Southern African Journal of Anaesthesia and Analgesia*

Lockaht R “Social Media and the Protection of Personal Information Act” 2021 *Southern African Journal of Anaesthesia and Analgesia* 569-572

Madon 2000 *Information Technology and People*

Madon S “The Internet and Socio-Economic Development: Exploring the Interaction” 2000 *Information Technology and People* 85-101

Martin and Zimmerman 2024 *Current Opinion in Psychology*

Martin KD and Zimmerman J “Artificial Intelligence and its Implications for Data Privacy” 2024 *Current Opinion in Psychology* 1-6

Mbonye and Moodley 2024 *South African Journal Information Management*

Mbonye V and Moodley K “Examining the Applicability of the Protection of Personal Information Act in AI-Driven Environments” 2024 *South African Journal Information Management* 1-8

Marelli 2024 *International Data Privacy Law*

Marelli M “Transferring Personal Data to International Organizations under the GDPR: An Analysis of the Transfer Mechanisms” 2024 *International Data Privacy Law* 19-36

Mantelero 2021 *Computer Law and Security Review*

Mantelero A “The Future of Data Protection: Gold Standard vs. Global Standard” 2021 *Computer Law and Security Review* 1-7

Marnewick and Bekker 2022 *Journal of Contemporary Management*

Marnewick C and Bekker G "Projectification within a Developing Country: The Case of South Africa" 2022 *Journal of Contemporary Management* 1-17

McQuoid-Mason 1982 *CILSA*

McQuoid-Mason DJ "Consumer Protection and the Right to Privacy" 1982 *CILSA* 135-157

Molnar 2024 *Regional Law Review*

Molnar D "I Unleashed: Mastering the Maze of the EU AI Act" 2024 *Regional Law Review* 155-168

Moseson et al 2022 *Plos One*

Moseson H et al "It Just Seemed Like a Perfect Storm": A Multi-Methods Feasibility Study on the Use of Facebook, Google Ads, and Reddit to Collect Data on Abortion-Seeking Experiences from People who Considered but Did Not Obtain Abortion Care in the United States" 2022 *Plos One* 1-14

Mtuze "Electronic Contracts(E-contracts) and E-commerce"

Mtuze SS "Electronic Contracts(E-contracts) and E-commerce" in Mtuze SS and Papadopoulos S (eds) *Cyberlaw@SA The Law of the Internet in South Africa* (Van Schaik Publishers Pretoria) 41-71

Mtuze and Papadopoulos *"*Privacy and Data Protection"

Mtuze SS and Papadopoulos S *"*Privacy and Data Protection" in Mtuze SS and Papadopoulos S (eds) *Cyberlaw@SA The Law of the Internet in South Africa* (Van Schaik Publishers Pretoria) 307-377

Mupangavanhu 2012 *PER/PELJ*

Mupangavanhu Y *"*An Analysis of the Dispute Settlement Mechanism Under the Consumer Protection Act 68 of 2008" *PER/PELJ* 2012 319-346

Mupangavanhu and Kerchhoff 2023 *De Jure*

Mupangavanhu Y and Kerchhoff D "Online Deceptive Advertising and Consumer Protection in South Africa – The law and Its Shortcomings?" 2023 *De Jure* 86-106

Nadhom and Loskot 2018 *Journal of Data in Brief*

Nadhom M and Loskot P "Survey of Public Data Sources on the Internet Usage and Other Internet Statistics" 2018 *Journal of Data in Brief* 1914-1929

Nagel et al *Commercial Law*

Nagel et al *Commercial Law* 6th ed (LexisNexis Pretoria 2018)

Naudé 2007 *SALJ*

Naudé T “The use of Black and Grey Lists in Unfair Contract Terms Legislation in Comparative Perspective” 2007 *SALJ* 128-164

Naudé 2017 *TSAR*

Naudé T “Towards augmenting the list of prohibited contract terms in the South African Consumer Protection Act 68 of 2008” 2017 *TSAR* 138-148

Naudé and Eiselen S “Introduction and Overview of the Consumer Protection Act”

Naudé T & Eiselen S “Introduction and Overview of the Consumer Protection Act” in Naudé T and Eiselen s (eds) *Commentary in the Consumer Protection Act* (Juta Claremont 2014) 1-21

Naudé and De Stadler Section 3”

Naudé T and De Stadler “Section 3” in Naudé T and Eiselen S (eds) *Commentary in the Consumer Protection Act* (Juta Claremont 2014) ch 3

Neethling 2008 *SALJ*

Neethling J “The Right to Privacy, HIV/AIDS and Media Defendants” 2008 *SALJ* 36-46

Neethling and Potgieter *Law of Delict*

Neethling J and Potgieter JM *Law of Delict* 7th edition (LexisNexis 2017)

Netshakhuma 2019 *Good Knowledge, Memory and Communication*

Netshakhuma NS “Assessment of a South Africa National Consultative Workshop on the Protection of Personal Information Act” 2019 *Good Knowledge, Memory and Communication* 58-74

Nguyen et al 2023 *Applied Sciences*

Nguyen T et al “A Study on Exploring the Level of Awareness of Privacy Concerns and Risks” 2023 *Applied Sciences* 1-13

Okpaluba 2015 *Acta Juridica*

Okpaluba C "Constitutional Protection of the Right to Privacy: The Contribution of Chief Justice Langa to the Law of Search and Seizure" 2015 *Acta Juridica* 407-429

Olaniran and Williams *Social Media Effects*

Olaniran B and Williams I *Social Media Effects: Hijacking Democracy and Civility in Civic Engagement. Platforms, Protests, and the Challenge of Networked Democracy* (SpringerNature Germany Berlin 2020)

Olimid 2024 *Access to Justice in Eastern Europe*

Olimid AP et al “Legal Analysis of EU Artificial Intelligence Act (2024): Insights from Personal Data Governance and Health Policy” 2024 *Access to Justice in Eastern Europe* 1-23

Ooijen and Vrabec 2019 *Journal of Consumer Policy*

Ooijen I and Vrabec HU “Does the GDPR Enhance Consumers’ Control over Personal Data? An Analysis from a Behavioural Perspective” 2019 *Journal of Consumer Policy* 91-107

Oyewole et al *Computer Science & IT Research Journal*

Oyewole AT et al “Data Privacy Laws and Their Impact on Financial Technology Companies: A Review” 2024 *Computer Science & IT Research Journal* 628-650

Papadopoulos 2009 *Obiter*

Papadopoulos S “Revisiting the Public Disclosure of Private Facts in Cyberworld” 2009 *Obiter* 30-43

Papadopoulos An Introduction to Cyberlaw”

Papadopoulos S “An Introduction to Cyberlaw” in Mtuze SS and Papadopoulos S (eds) *Cyberlaw@SA The Law of the Internet in South Africa* (Van Schaik Publishers Pretoria) 1-8

Papadopoulos 2022 *THRHR*

Papadopoulos S "The Long Road to Mastering the POPIA: Lessons from Sheburi v Railway Safety Regulator - Sheburi v Railway Safety Regulator GATW 15200-21 (CCMA, 2 March 2022)" 2022 *THRHR* 397-408

Pelteret and Ophoff 2016 *Informing Science:* The International Journal of Emerging *Transdiscipline*

Pelteret M and Ophoff J “A Review of Information Privacy and its Importance to Consumers and Organizations” 2016 *Informing Science:* The International Journal of Emerging *Transdiscipline* 277-301

Peté *Civil Procedure: A Practical Guide*

Peté S *Civil Procedure: A Practical Guide* 3rd ed (Oxford University Press Southern Africa Cape Town 2016)

Phiri 2023 *Law, Democracy and Development*

Phiri S “The right of Access to Information vs the Right to Privacy in *Tiso Blackstar Group (Pty) Ltd & Others v Steinhoff International Holdings*

N.V. (18706/2019) [2022] ZAWCHC 265" 2023 *Law, Democracy and Development* 266-275

Pierce "Electronic Communications Regulation in South Africa"

Pierce L "Electronic Communications Regulation in South Africa" in Mtuze SS and Papadopoulos S (eds) *Cyberlaw@SA The Law of the Internet in South Africa* (Van Schaik Publishers Pretoria) 11-37

Quinn and Malgieri 2020 *German Law Journal*

Quinn P and Malgieri G "The Difficulty of Defining Sensitive Data – The Concept of Sensitive Data in the EU Data Protection Framework" 2020 *German Law Journal* 1-31

Rautenbach 2001 *Journal of South African Law*

Rautenbach IM "The Conduct and Interests Protected by the Right to Privacy in Section 14 of the Constitution" 2001 *Journal of South African Law* 115-123.

Reddy-Girad 2017 *International Law News*

Reddy-Girad D "French Data Protection Rules" 2017 *International Law News* 11-14

Robinson 2014 *THRHR*

Robinson JA 2014 "The Overlap Between the Consumer Protection Act 68 of 2008 and the National Credit Act 34 of 2005: A Comparison with Australian Law" *THRHR* 135-144

Rose 2021 *Brooklyn Journal of Corporate, Financial & Commercial Law*

Rose B "The Commodification of Personal Data and the Road the Commodification of Personal Data and the Road to Consumer Autonomy through the CCPA to Consumer Autonomy through the CCPA" 2021 *Brooklyn Journal of Corporate, Financial & Commercial Law* 521-542

Ruohonen and Hjerppe 2021 *Information Systems*

Ruohonen J and Hjerppe K "The GDPR Enforcement Fines at Glance" 2021 *Information Systems* 1-9

Roos 2006 *Comparative and International Law Journal of South Africa*

Roos A 2006 "Core Principles of Data Protection Law" 2006 *Comparative and International Law Journal of South Africa* 102-130

Roos 2023 *THRHR*

Roos A 2023 "Data Protection Principles under the GDPR and the POPI Act: A Comparison" *THRHR* 1-26

Saheb 2023 *AI and Ethics*

Saheb T “Ethically Contentious Aspects of Artificial Intelligence Surveillance: A Social Science Perspective” 2023 *AI and Ethics* 369-379

Sai 2024 *International Journal of Law Management & Humanities*

Sai K “Digital Data Protection Act, 2023” 2024 *International Journal of Law Management & Humanities* 1053-1071

Samonte 2019 *European Papers-A Journal on Law and Integration*

Samonte M “Google v. CNIL: The Territorial Scope of the Right to be Forgotten under EU Law” 2019 *European Papers-A Journal on Law and Integration* 839-851

Saurabh 2024 *International Journal of Law in Changing World*

Saurabh S “The Digital Personal Data Protection Act of 2023: Strengthening Privacy in the Digital Age” 2024 *International Journal of Law in Changing World* 77-94

Schemer et al 2021 *Journal of Computer-Mediated Communication*

Schemer C et al “The Impact of Internet and Social Media Use on Well-Being: A Longitudinal Analysis of Adolescents Across Nine Years” 2021 *Journal of Computer-Mediated Communication* 1-16

Schultz and Freedman 2023 *PER/PELJ*

Schultz H and Freedman W “Plugins and POPI: A Critical Discussion into the Legal Implications of Social Plugins and the Protection of Personal Information” 2023 *PER/PELJ* 1-27

Seetharamu et al 2024 *International Journal of Scientific Research in Science, Engineering and Technology*

Seetharamu S et al “Digital Data Protection Laws: A Review” 2024 *International Journal of Scientific Research in Science, Engineering and Technology* 64-75

Shanapinda 2019 *The African Journal of Information and Communication*

Shanapinda S “Asymmetry in South Africa’s Regulation of Customer Data Protection: Unequal Treatment Between Mobile Network Operators (MNOs) and over-the-top (OTT) Service Providers” 2019 *The African Journal of Information and Communication* 1–20

Sharma 2023 *International Journal of Law Management and Humanities*

Sharma A “Transforming Data Privacy: An Analysis of India's Digital Personal Data Protection Act” 2023 *International Journal of Law Management and Humanities* 1841-1853

Sharma 2024 *Futures*

Sharma S “Benefits or Concerns of AI: A multistakeholder Responsibility” 2024 *Futures* 1-8

Swales 2022 *PER/PELJ*

Swales L “The Protection of Personal Information Act 4 of 2013 in the Context of Health Research: Enabler of Privacy Rights or Roadblock?” 2022 *PER/PELJ* 783- 797

Swales 2021 *South African Journal of Science*

Swales L “The Protection of Personal Information Act and Data De-identification” 2021 *South African Journal of Science* 1-3

Solove 2023 *Notre Dame Law Review*

Solove DJ “The Limitation of Privacy Rights” 2023 *Notre Dame* 977-1034

Solove and Schwartz *EU Data Protection and the GDPR: [Connected EBook]*

Solove DJ and Schwartz PM *EU Data Protection and the GDPR: [Connected EBook]* (Aspen Publishing United States Boston)

Swales et al 2022 *South African Journal of Science*

Swales L et al “Why Research Institutions Should Indemnify Researchers Against POPIA Civil Liability” 2022 *South African Journal of Science* 1-3

Swales 2016 *SA Merc LJ*

Swales L “Protection of personal information: South Africa's Answer to the global Phenomenon in the Context of Unsolicited Electronic Messages (Spam)” 2016 *SA Merc LJ* 49-84

Syarah et al ” 2024 *International Journal of Religion*

Syarah MM et al “Adapting to the Digital Landscape: A Phenomenological Study of How Journalists Reshape Their Professional Identity and Practices” 2024 *International Journal of Religion* 7323-7336

Tambou 2019 *European Data Protection Law Review*

Tambou O “Lessons from the First Post-GDPR Fines of the CNIL against Google LLC” 2019 *European Data Protection Law Review* 80-84

Tambou 2018 *European Data Protection Law Review*

Tambou O “France: The French Approach to the GDPR Implementation” 2018 *European Data Protection Law Review* 88-94

Tomada 2022 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*

Tomada L “Start-ups and the Proposed EU AI Act: Bridges or Barriers in the Path from Invention to Innovation?” 2022 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 53-66

Trabelsi 2024 *Journal of Electronic Business and Digital Economics*

Trabelsi MA “The Impact of Artificial Intelligence on Economic Development” 2024 *Journal of Electronic Business and Digital Economics* 142-153

Turoń and Kubik 2021 *Journal of Open Innovation Technology Market and Complexity*

Turoń K and Kubik A “Business Innovations in the New Mobility Market during the COVID-19 with the Possibility of Open Business Model Innovation” 2021 *Journal of Open Innovation Technology Market and Complexity* 1-21

Tladi and Papadopoulos “Consumer Protection in E-Commerce”

Tladi S and Papadopoulos S “Consumer Protection in E-Commerce” in Mtuze SS and Papadopoulos S (eds) *Cyberlaw@SA The Law of the Internet in South Africa* (Van Schaik Publishers Pretoria) 75-138

van der Merwe 2023 *Obiter*

van der Merwe DP “Legal Aspects of the Fourth Industrial Revolution (4ir) – (with Specific Reference to ChatGPT and other Software Purporting to Give Legal Advice)” 2023 *Obiter* 939-959

Van Dokkum 1996 *South African Journal of Criminal Justice*

Van Dokkum N "Medical Evidential Privilege" 1996 *South African Journal of Criminal Justice* 14-21

Van Heerden “Section 69”

Van Heerden C “Section 69” in in Naudé T and Eiselen s (eds) *Commentary in the Consumer Protection Act* (Juta Claremont 2014) ch 69

van Norren 2022 *Journal of Information, Communication and Ethics in Society*

van Norren D “The Ethics of Artificial Intelligence, UNESCO and the African Ubuntu Perspective” 2022 *Journal of Information, Communication and Ethics in Society* 112-128

Vandezande 2019 *International Journal for the Data Protection Officer, and Privacy Counsel*

Vandezande “An Update on GDPR Fines in Belgium” 2019 *International Journal for the Data Protection Officer, and Privacy Counsel* 17-19

Verhoef 2019 *Journal of Business*

Verhoef PC et al “Digital Transformation: A Multidisciplinary Reflection and Research Agenda” 2019 *Journal of Business* 889-901

Kolfschooten and Oirschot 2024 *Health Policy*

van Kolfschooten H and van Oirschot J “The EU Artificial Intelligence Act (2024): Implications for Healthcare” 2024 *Health Policy* 1-4

Van Heerden and Barnard 2011 *Journal of International Commercial Law and Technology*

Van Heerden and J Barnard J “Redress for Consumers in Terms of the Consumer Protection Act 68 of 2008: A Comparative Discussion” 2011 *Journal of International Commercial Law and Technology* 131-144

Van Heerden “Section 69”

Van Heerden C “Section 69” in Naudé T and Eiselen S (eds) *Commentary on the Consumer Protection Act* (Juta Claremont 2014) ch 69

Wald 1983 *Maryland Law Review*

Wald PM “The Problem with the Courts: Black-Robed Bureaucracy, or Collegiality under Challenge” 1983 *Maryland Law Review* 766-786

Wachter 2024 *Yale Journal of Law & Technology*

Wachter S “Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond” 2024 *Yale Journal of Law & Technology* 674-718

Woker 2019 *Stell LR*

Woker T “Consumer protection: An Overview Since 1994” 2019 *Stell LR* 97-115

Woker 2017 *SA Merc LJ*

Woker T “Evaluating the Role of the National Consumer Commission in Ensuring That Consumers Have Access to Redress” 2017 *SA Merc LJ*1-16

Woker 2010 *Obiter*

Woker T “Why the Need for Consumer Protection Legislation? A look at some of the Reasons Behind the Promulgation of The National Credit Act and The Consumer Protection Act” 2010 *Obiter* 217 – 231

Williams 2007 *Journal of Business and Economic Research*

Williams C “Research Methods” 2007 *Journal of Business and Economic Research* 65-71

Zeisel and Callahan 1963 *Harvard Law Review*

Zeisel H and Callahan T “Split Trials and Time Saving: Statistical Analysis” 1963 *Harvard Law Review* 1606-1625.

Zenda et al 2020 *South African Computer Journal*

Zenda B et al “Protection of Personal Information: An experiment Involving Data Value Chains and the use of Personal Information for Marketing Purposes in South Africa” 2020 *South African Computer Journal* 113–132.

Case Law

AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others [2021] ZACC 3

Bernstein and Others v Bester NO and Others (CCT23/95) [1996] ZACC 2

Booi v Amathole District Municipality and Others (CCT 119/20) [2021] ZACC

Boxing South Africa v Qithi (Leave to Appeal) [2022] JOL 56302 (LC)

De Jager v Netcare Limited and Others (42041/16) [2025] ZAGPPHC 141

De Jager v Netcare Limited [2024] JOL 65458 (GP)

Chirwa v Transnet Ltd & others [2008] 2 BLLR 97 (CC)

Government of the Republic of South Africa and Others v Grootboom and Others 2001 (1) SA 46

Kelter Presentations v Internet Service Providers' [2014] JOL 31136 (GSJ)

Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others (CCT1/00) [2000] ZACC

Janse Van Rensburg NO v Minister of Trade and Industry 2001 1 SA 29 CC

Jansen van Vuuren and Another NNO v Kruger [1993] 2 All SA 619 (A)

Joroy 4440 CC t/a Ubuntu Procurement v Potgieter N.O. and Another 2016 (3) SA 465 (FB)

Mukaddam v Pioneer Foods (Pty) Ltd and Others (CCT 131/12) [2013] ZACC 23

National Media Ltd v Jooste 1996 (3) SA 262 (SCA)

S v J [2011] 2 All SA 299 (SCA)

S v Matomela [1998] 2 All SA 1 (Ck)

S v Makwanyane and Another 1995 (3) SA 391

S v Pepsi-Cola (Pty) Ltd 2985 2 SA 141 (C)
Magidiwana and other injured and arrested persons v President of the Republic of South Africa and others (No 2) [2013] ZAGPPHC 292 (GNP)
NM and Others v Smith and Others (Freedom of Expression Institute as Amicus Curiae) 2007 (5) SA 250 (CC)
Nkuzi Development Association v Government of the Republic of South Africa and Another [2001] 4 All SA 460 (LCC)

Foreign Case Law

Employees' Retirement System of Rhode Island, et. al. v. Mark Zuckerberg, et al. and City of Warwick Retirement System et. 2021-0617-JRS
Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, Court of Justice of the European Union (CJEU) C-311/18
IAB Europe v Gegevensbeschermingsautoriteit C-604/2
Data Protection Commissioner v Facebook Ireland and Maximillian Schrems C-311/18
Meta vs Bundeskartellamt C-252/21
United States of America v Facebook Inc. 456 F. Supp. 3d 105 (D.D.C. 2020)
Google LLC v. Commission Nationale de l'informatique et des libertés (CNIL) 2019 ECJ C 507

Legislation

Constitution of the Republic of South Africa, 1996
Consumer Protection Act 68 of 2008
Electronic Communications and Transactions Act 25 of 2002
Protection of Personal Information Act 4 of 2013
Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002

Foreign Legislation

AI Act
Digital Personal Data Protection Act 2023
French Data Protection Act No 78-17 of 1978
Federal Data Protection Act 30 of 2017
General Data Protection Regulation (EU) 2016/679

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1981

Internet Sources

South African property giant hit by major data breach

"South African property giant hit by major data breach" 2024 available at https://businesstech.co.za/news/property/816277/warning-over-property-data-breach-in-south-africa/

Admire *Cyber attack rattles real estate firm Pam Golding* https://www.itweb.co.za/article/cyber-attack-rattles-real-estate-firm-pam-golding/lLn14MmQoLwMJ6Aa

Admire M "Cyber attack rattles real estate firm Pam Golding" 2024 available at https://www.itweb.co.za/article/cyber-attack-rattles-real-estate-firm-pam-golding/lLn14MmQoLwMJ6Aa

AI National Government Summit Discussion Document: South Africa's Artificial Intelligence (AI) Planning: Adoption of AI by Government https://www.dcdt.gov.za

Department of Communications and Digital and Digital Technologies "AI National Government Summit Discussion Document: South Africa's Artificial Intelligence (AI) Planning: Adoption of AI by Government"2023 available at https://www.dcdt.gov.za/images/phocadownload/AI_Government_Summit/National_AI_Government_Summit_Discussion_Document.pdf

Annual Report for 2023/24 Financial Year for the Information Regulator https://inforegulator.org.za/wp-content/uploads/2020/07/Information-Regulator-Annual-Report-2023_25_Approved-by-Members_Final90.pdf

Information Regulator "Annual Report for 2023/24 Financial Year for the Information Regulator" 2024 available at https://inforegulator.org.za/wp-content/uploads/2020/07/Information-Regulator-Annual-Report 2023_25_Approved-by-Members_Final90.pdf

Information Regulator Annual Report For the Year Ended 31 March 2023 https://inforegulator.org.za/wp-content/uploads/2020/07/Information-Regulator-Annual-Report-2023-Compressed.pdf

Information Regulator "Information Regulator Annual Report For the Year Ended 31 March 2023" 2023 available at https://inforegulator.org.za/wp-

content/uploads/2020/07/Information-Regulator-Annual-Report-2023-Compressed.pdf

South Africa National Artificial Intelligence Policy Framework https://www.dcdt.gov.za/sa-national-ai-policy-framework/file/338-sa-national-ai-policy-framework.html

Department of Communications and Digital Technologies “South Africa National Artificial Intelligence Policy Framework” 2024 available at https://www.dcdt.gov.za/sa-national-ai-policy-framework/file/338-sa-national-ai-policy-framework.html

Government Publication

GN 2798 in GG 51436 of 28 October 2024