UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG | WITS SCHOOL OF LAW

THE PROTECTION OF PERSONAL INFORMATION ACT: A CRITIQUE THROUGH THE LENS OF LIBERTARIAN LEGAL THEORY

By

Jonathan Alan Meyer

542555

Under the supervision of

Prof. Emile Zitzke

Submitted in partial fulfilment of the requirements for the degree of

Master of Laws by Coursework and Research Report

at the University of the Witwatersrand, Johannesburg

Date: 31 October 2022

DECLARATION

I declare that this report is my own, unaided work. It is submitted in partial fulfilment of the requirements for the degree of Master of Laws in the field of Commercial and Business Law at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any other degree or examination in any other university.

_____

542555

31 OCTOBER 2022

ABSTRACT

This paper offers a critical analysis of the Protection of Personal Information Act 4 of 2013 (POPIA) and its impact on freedom of trade, occupation and profession (freedom of trade) as found under s 22 of the Bill of Rights in the Constitution of the Republic of South Africa, 1996 (the Constitution) from a libertarian legal theory perspective. Owing to a lacuna in South African law, the provisions of POPIA that seem to impede free trade will probably not result in an unconstitutional infringement of the section 22 right. Those provisions in POPIA that restrict free trade may nevertheless be critiqued from the perspective of libertarian legal theory. More specifically, libertarian legal theory's rejection of over-regulation. In this research report, the ultimate finding is that the cardinal issue with POPIA is that, paradoxically, and despite POPIA's proclamation to promote a free-flow of information in balancing such purpose with the Constitutional right to privacy found under s 14 of the Constitution, POPIA serves to limit, over-restrictively, the free flow of information between businesses and business, and businesses and natural persons. The research report conducts a cursory analysis of the right of freedom of trade and investigates certain important provisions of POPIA through a libertarian-legal lens. There are three weaknesses in POPIA that are identified in this research report. Firstly, POPIA has a negative impact on trade because both natural and juristic persons receive data protection in terms of the Act, whereas in jurisdictions where the GDPR operates, only natural persons receive such protection. It will be shown how this aspect of POPIA is potentially overly onerous on businesses. Secondly, the security requirements under POPIA are not only unreasonably onerous on, and expensive for, companies, to implement, but they are cumbersome, contradictory and vague. It will be shown how this could negatively affect free trade. Thirdly, POPIA's sections dealing with civil liability are too far-reaching in their consequences of business, while also providing for defences to responsible parties which are prejudicial to data subjects. This amounts to an over-regulation, which is antithetical to libertarian legal theory.

TABLE OF CONTENTS

1. INTRODUCTION

The Constitution of the Republic of South Africa, 1996 provides the framework for which legislation ought to be enacted – it stipulates the rights which ought to protected, with enabling legislation being promulgated to give life to these recognised human rights.[1] The purpose of the Protection of Personal Information Act (POPIA)[2] is, amongst other things, to 'give effect to the constitutional right to privacy',[3] enshrined in section 14 of the Constitution, while securing a balance between privacy rights and competing rights under the Constitution.[4] It is understood that any attempt by the legislature to balance the competing constitutional rights[5] is a difficult task, especially as no rights under the Constitution are deemed — without justification under s 36 of the Constitution — more important than the others.[6] One of the rights that compete with the right to privacy is that of freedom of trade, occupation, and profession (hereafter "freedom of trade"), enshrined in section 22 of the Constitution.

This research report will argue that POPIA contains certain provisions that limit freedom of trade in ways that would be regarded as repugnant to a libertarian-minded lawyer. This is so because POPIA has certain negative effects on the free market and, by extension – I will argue – the right to freedom of trade. This research report will primarily involve a libertarian jurisprudential critique of POPIA. To conduct this libertarian critique, this report will commence by exposing inconsistencies within POPIA to highlight the damaging effects that POPIA will have on the free market. The research report will proceed, in Part 2, with a brief analysis of the competing rights to privacy and freedom of trade, and the lack of protection offered to juristic persons under s 22 of the Constitution. Using libertarian legal theory as a premise, in Part 3 it will be argued that POPIA should not apply to juristic persons as data subjects. Such an exposé will be attempted by tracing the history of informational privacy in SA, briefly investigating definitions under the Promotion of Access to Information Act,[7] and by

[1] *S v Mhlungu and Others* 1995 (3) SA 867 (CC) para 69.
[2] Protection of Personal Information Act 4 of 2013.
[3] Section 2(a) of POPIA.
[4] Ibid s 2(a)(*i*).
[5] Ibid.
[6] *Islamic Unity Convention v Independent Broadcasting Authority* 2002 (4) SA 294 (CC) para 30. See also *De Reuck v Director of Public Prosecutions Witwatersrand Local Division and Others* 2004 (1) SA 406 (CC) para 55.
[7] Promotion of Access to Information Act 2 of 2000 (hereinafter referred to as PAIA).

comparing POPIA's inclusion of juristic persons as data subjects with the General Data Protection Regulation's[8] rejection of such inclusion.

Thereafter, in Part 4 the research report will demonstrate ways in which the provisions of POPIA amount to an over-regulation through an overview of the security provisions found under POPIA. The security provisions will be highlighted in an attempt to reveal how they are both confusing and that, in practice, they will prove to be unnecessarily burdensome on businesses. This will be conducted through a criticism of the use of the word 'reasonable' in relation to security requirements and through a discussion on market-regulation. On this point, the paper will also contrast the GDPR's security requirements and POPIA's security requirements. It will ultimately be shown that libertarian legal theory would balk at POPIA's overregulated security provisions.

The paper will continue, in Part 5 with an exposition of issues arising out of civil claims under POPIA, such as: the debate surrounding strict liability; the absence of an escape from vicarious liability; the problem with POPIA's stated defences against civil claims; and the misplacement of the concept of aggravated damages as a remedy in the Act. It will be argued under this civil-claims section of the research report that, in addition to how the onerous security requirements under POPIA act to stifle trade, and thus freedom of trade, the issues surrounding liability under POPIA act to solidify the concerns of businesses in SA and further detract from a free market.

2. FREEDOM OF TRADE, LIBERTARIANISM AND THE RIGHT TO PRIVACY

2.1. THE FREEDOM OF TRADE DEFICIT

"Every citizen has the right to choose their trade, occupation or profession freely. The practice of a trade, occupation or profession may be regulated by law."[9] Davis opines that this constitutional right to trade must be understood as a legal construct to provide corrective measures to apartheid employment inequalities.[10] Indeed, in *JR*

[8] EU General Data Protection Regulation (GDPR): Regulation EU 2016/679 (hereinafter referred not as 'the GDPR').
[9] Section 22 of the Constitution.
[10] D Davis 'Freedom of Trade, Occupation and Profession' in Stuart Woolman et al (eds) *Constitutional Law of South Africa* 2 ed (Service 12-03) 54-2.

Investments 1013[11] it was noted that s 22 of the Constitution was designed specifically for, inter alia, extending the predominantly white-centric structures which had been implemented for the development of the training and skills in the employment sphere to include black individuals.[12]

However, the right to freedom of trade is not unlimited and may be regulated by law.[13] The regulation permitted in the second sentence of s 22 of the Constitution, however, does not entail that a statute such as POPIA may regulate freedom of trade in general, but rather that the government has the power to reasonably restrict the practice of a 'particular trade' or profession.[14] In other words, the restriction of the exercise of trade ought to be 'necessary or desirable'.[15] For, the right to freedom of trade is closely related to, and informs, the economic growth and the flourishing of the SA economy[16] on the one hand, and from an equality perspective, as an inclusive and non-discriminatory economy, on the other hand.[17] Were the provisions of POPIA to stifle economic growth, it stands to reason that the persons who would be worst affected, economically, would be previously-disadvantaged South Africans.

A further limitation to the right to trade is that, historically, the right was only afforded to (natural person) citizens,[18] as opposed to being afforded to both natural and juristic persons. This was confirmed in the case of *Mukaddam v Pioneer Foods,*[19] where the Nugent JA held that to extend the right to freedom of trade to juristic persons would be anti-competitive and that juristic persons have no constitutional remedies against being unprofitable, or against economic failure.[20] Although the order of the Supreme Court of Appeal[21] was overturned in the Constitutional Court, the Constitutional Court confirmed the Supreme Court of Appeal judgment in so far as it

[11] *JR 1013 Investments CC and Others v Minister of Safety and Security and Others* 1997 (7) BCLR 950 (E).
[12] Ibid at 980B-E.
[13] Section 22 of the Constitution.
[14] *Van Rensburg v South African Post Office Ltd* 1998 (10) BCLR 1307 (E) at 1322E.
[15] Ibid at 1307E.
[16] For example, the Black Industrialist Scheme was introduced by the Department of Trade and Industry to assist previously disadvantaged persons in entering the 'industrial base' (trade / occupation), for the purposes of economic growth; see *Minister of Trade and Industry & Another v Murendi Properties and Building Supplies (Pty) Ltd* [2021] ZASCA 53 para 2.
[17] Catherine Albertyn & Beth Goldblatt 'Equality' in Stuart Woolman et al (eds) *Constitutional Law of South Africa* 2 ed (Service 12-03) 35-4.
[18] Davis op cit note 10 at 54-2.
[19] *Mukaddam v Pioneer Foods (Pty) Ltd and Others* 2013 (2) SA 254 (SCA).
[20] Ibid para 8.
[21] Ibid.

related to the limited application of the right to trade.[22] To date, the extension of the right to juristic persons applies only in so far as is relates to the protection of the rights of employees,[23] and such true extension has not found form other than in an obiter dictum.[24] The notional difficulty with the application of the right of freedom of trade, exclusively to natural persons is that, indirectly, natural persons stand to suffer due to juristic persons not being afforded a constitutional right to trade.[25] For example, natural persons require the employment opportunities offered by juristic persons. Hence, it is argued that to give true effect to s 22 of the Constitution, freedom of trade should be extended to juristic persons, together with many other rights under the Bill of Rights which are afforded to juristic persons.

Section 8(4) of the Constitution provides for instances in which the rights protected under the Bill of Rights may be extended to juristic persons, as and when may be necessary. Our courts have recognised that privacy, as found under s 14 of the Constitution, applies both to natural and juristic persons.[26] This begs the question how this inconsistency (between privacy and freedom of trade) within the Constitution is justified. Under the Constitution, a juristic person is denied the right to freedom of trade, but upon trading, a juristic person's right to privacy is tantamount to the natural person's right to trade as both the rights to trade and of privacy of a natural person are contingent on a juristic person employer being afforded the right to trade. For, without a juristic person being able to trade, no privacy rights would exist to require protection. The rights found in the Bill of Rights are interrelated, thus it would appear incompatible that one component of these inter-related rights (the right to trade) applies to natural persons only, and that another component (the right of privacy) applies both to natural and juristic persons.

While various limitations of POPIA on the right to trade are neither desirable nor necessary, it cannot be argued that the limitations result in an unconstitutional[27] infringement on freedom of trade as freedom of trade has not been extended to juristic

[22] *Mukaddam v Pioneer Foods (Pty) Ltd and Others* 2013 (5) SA 89 (CC) para 71.
[23] *Contract Employment Contractors (Pty) Ltd v Motor Industry Bargaining Council (MIBCO) and Others* 2013 (3) SA 308 (LC) para 23.
[24] Ibid para 22.
[25] Ibid para 23.
[26] *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* 2001 (1) SA 545 (CC) para 17.
[27] *Van Rensburg* supra note 14 at 1307E.

persons. However, libertarian legal theory requires law to be necessary and desirable, and for that reason, the provisions of POPIA will be analysed from a libertarian legal theory perspective.

2.2. LIBERTARIANISM

Libertarianism, or a free-market approach,[28] is an ideology which recognises as sacrosanct, the importance of individual freedom, private liberty and property rights in law, politics and governance.[29] Libertarian governance is reflected by self-determination[30] - for self and for others.[31] From a strictly legal perspective, libertarian laws and public policy are founded on the notion of individual freedom, to the exclusion of overbearing government interference. Libertarianism – or at least minarchist libertarianism– does not reject the influence or importance of public policy, history and culture on the law, but rather, libertarian legal theory is concerned with individual liberty in so far as it relates to 'the social nature of humanity'.[32]

According to Hospers, libertarianism deems victims of harm worthy of protection, and he defines harm to mean bodily injury, damage to property, theft, and a breach of contract[33] (which would include a social contract).[34] This is commonly referred to as the "non-aggression principle", whereby the laws should only be in place to protect corollary rights.[35] Simply put, libertarian legal theory incorporates the social nature of human beings.[36] People should be free to choose to interact with one another in a manner of their choosing,[37] with the result being developing sustainable, stable and voluntary associations within communities.[38] Indeed, libertarianism does not require being totally unruled, but that one has the freedom to conduct oneself in such a manner which does not infringe on the rights (and thus freedoms) of another.[39] In effect, the libertarian legal theory would promote and support – and thus informs –

[28] M van Staden 'Spontaneous Order or Central Planning? A brief overview of the Libertarian Approach to Law' (2021) 84 *THRHR* 53 at 66.
[29] Ibid 53-4.
[30] Croley, S.P. 'Libertarianism as Critical Theory' (1996) 1 *Michigan Law and Policy Review* 179 at 180.
[31] Van Staden op cit note 28 at 54.
[32] Ibid.
[33] J Hospers 'Libertarianism and legal paternalism' (1980) 4(3) *Journal of Libertarian Studies* 261.
[34] Van Staden op cit note 28 at 54.
[35] Ibid at 55-6.
[36] G Sartori 'Liberty and Law' (1976) 5 *Studies in Law*, Institute for Humane Studies 8.
[37] Croley op cite note 30 at 183-4.
[38] Van Staden op cit note 28 at 56.
[39] Ibid at 57.

freedom of trade as freedom of trade entails that social and *economic choices* are not restricted,[40] on condition that one's choices do not infringe the rights of others.[41] Likewise, freedom of trade entails that every person is entitled to choose their trade, occupation or profession[42] – *economic choices*. Further, both libertarian legal theory and the Bill of Rights impose limitations on the economic choices of persons, with libertarian legal theory limiting one's economic choices should such choices infringe the rights of others, and freedom of trade being limited by law, should the restriction be 'necessary or desirable',[43] and of course by other competing rights, subject to a s 36 limitations analysis.[44] Thus, both concepts give rise to freedom to trade, subject to necessary or desirable regulations which prevent the unreasonable infringement of other person's competing rights – or harm to other persons.

In SA, harm caused by invasions of privacy are already safeguarded by the common law. For example, in the case of *NM v Smith*,[45] the second respondent obtained a copy of the subjects' sensitive personal information. However, the subjects were not party to the terms governing the processing of their information and thus their privacy rights were protected through an award for damages.[46] In terms of protections offered to juristic persons, the courts have recognised the public interest in preserving the confidentiality of private occurrences and in preventing the dissemination of unlawfully obtained 'private and confidential information, to the media'.[47] This author argues that there exists a moral basis for protecting juristic persons' confidential information.

The moral authority of the law ought to be self-evident; the legislature must promulgate legislation based on extra-legal facts.[48] For example, POPIA's relevance in protecting data rights[49] is necessary in a world where personal data large swathes of the global population have subscribed to social media services and their personal data are being used by tech companies whereby natural persons become the product

[40] Croley op cite note 30 at 181.
[41] Van Staden op cit note 28 at 57.
[42] Section 22 of the Constitution.
[43] *Van Rensburg* supra note 14 at 1307E.
[44] *South African Human Rights Commission v Qwelane; Qwelane v Minister for Justice and Correctional Services* 2018 (2) SA 149 (GJ) para 53.
[45] *NM & others v Smith & others* 2007 (5) SA 520 (CC).
[46] Ibid para 15.
[47] *Sage Holdings Limited v Financial Mail (Pty) Limited* 1993 (2) SA 451 (AD) at 37.
[48] Van Staden op cit note 28 at 58.
[49] Section 2(*a*) of POPIA.

whose information is sold to tech companies for marketing purposes – thus the commodification of the natural person and his/her data.[50] Additionally, the importance of s 12 of ECTA[51] (which recognises the importance of data messages as a form of 'writing') is self-evident in a world where more and more formal communications – especially for the purpose of commerce – are being transmitted via data message. In short, the protection of data through law is something that libertarian legal theory can support, in principle. However, the finer details of SA's manner of protecting data through law is where the libertarian lawyer would start objecting.

Additionally, according to Hayek, law is, when stripped down to its core, common law (both criminal and civil).[52] The legislature should merely amend or revoke laws which require amendment and/or revocation to better protect individual liberty as the common law would bind and protect legal subjects.[53] We might refer to this principle as the 'anti-overregulation' principle. In the libertarian view, if legislative interventions are made, they ought not interfere unduly with one's economic choices (freedom of trade). In later parts of this research report, I will show that POPIA is harmful to businesses to such an extent that it is not only overly restrictive on commerce, but POPIA is overly restrictive on trade. As above, harm to a juristic person at the hands of privacy invasions are already protected by common law[54] and thus, POPIA's application to juristic persons as data subjects does not offer any additional protection to juristic persons (a point taken further in Part 3 of this research report below). In turn, it provides a strong argument in favour of libertarian legal theory: the law surrounding data protection, at least in so far as juristic persons are concerned, should be fluid, voluntarily formed and not directed by government, as will be explained below.

2.3. THE RIGHT TO PRIVACY

"Everyone has the right to privacy, which includes the right not to have […] the privacy of their communications seized."[55] In SA, the Constitution affords everyone the right to privacy under s 14 of the Bill of Rights. The law acts as a tool of protecting, and not

[50] A Roos 'Privacy in the Facebook Era: A South African Legal Perspective' (2012) 129 *SALJ* 375 at 383.
[51] Act 25 of 2002.
[52] T.R.S. Allan *Constitutional Justice: A liberal theory of the rule of law* (2001) 33.
[53] Ibid 38.
[54] See note 47 above.
[55] Section 14(*d*) of the Constitution.

creating, the right to privacy for it is in a person's innate interest to protect his privacy, much as it is in one's innate interest to protect his reputation, dignity, and so forth.[56] However, it is challenging to aptly define the notion of privacy as privacy is forever-changing and contains different meanings to different people, and across changing situations.[57] In *Financial Mail v Sage*,[58] two forms of privacy were recognised: (1) an unlawful intrusion (substantive privacy); and (2) unlawful disclosure of facts (informational privacy).[59] In *Bernstein v Bester*,[60] Ackermann J opined that as no right is absolute, the right to privacy is limited to 'family life, sexual preference and home environment', that is, the 'inner sanctum of a person' (or substantive privacy).[61] The Court went further to state that privacy is a subset of dignity and is understood to mean a 'seclusion from the public and publicity'.[62] Notably, such a narrow approach does not provide for the inclusion of informational privacy–the protection, as private, of information which is arguably not of a private nature, but rather of a factual nature.[63] In SA, informational privacy could be recognised as constituting a state of being safeguarded from, and having autonomy over, one's personal knowledge entering into, or remaining in, the public sphere.[64] Neethling's common-law understanding of (informational) privacy has filtered into constitutional privacy cases.[65] In *Bernstein*,[66] the right to (substantive) privacy was explained to extend to persons who had a legitimate expectation of privacy: the expectation of privacy ought to have been subjectively expected, and objectively reasonably.[67] For an expectation to be reasonable, the right to privacy entails that as information extends further from one's inner sanctum, and into the public sphere – including the business realm – privacy rights begin to diminish.[68] In *Hyundai*,[69] the need to extend the right of privacy to juristic persons was explicated as a defence by juristic persons against unlawful state

[56] J Neethling 'The concept of Privacy in South African Law' (2005) 122 *SALJ* 18 at 19.
[57] Ibid at 18.
[58] *Sage* supra note 47.
[59] Ibid at 30.
[60] *Bernstein v Bester* 1996 (2) SA 751.
[61] Ibid at 67.
[62] Ibid at 68.
[63] Neethling op cit note 56 at 20.
[64] Ibid at 19-20.
[65] *Smith* supra note 45 para 40.
[66] *Bernstein* supra note 60.
[67] Ibid para 75.
[68] Ibid para 67.
[69] *Hyundai* supra note 26.

searches and seizures on the juristic person's property.[70] Indeed, it appears not to have been the court's intention to extend informational privacy rights to juristic persons, for business dealings are far extended from the 'inner sanctum',[71] as referred to in *Bernstein*.[72] Due to juristic persons being unable to possess dignity or an inner sanctum, the conception of privacy differs from juristic person to natural person, with the latter's rights to privacy being more complete.[73] Notably, the reason postulated for extending privacy rights to juristic persons was to protect entities from unlawful state searches and seizures.[74] Thus, if we follow the anti-overregulation principle explained earlier, it appears that it should not have been the judiciary's intention to extend the right of informational privacy to juristic persons, with informational privacy otherwise being protected by South African courts through the common law.

However, as POPIA was promulgated to give effect to informational privacy, it is apposite to borrow from Roos, who postulates that informational privacy is the protection of a data subject's personal information or data from being processed by another natural or juristic person.[75] The importance of the right to informational privacy should be heralded, not only for its protection of human dignity,[76] but also due to the risks that technology brings to the processing of information: including but not being limited to inaccurate, incomplete, irrelevant or unlawfully obtained data,[77] with the latter also constituting an infringement of identity.[78]

With that being said, this author is of the view that certain provisions of POPIA will have a negative impact on commerce, thereby strengthening the libertarian legal theory argument against over-regulation, specifically in respect of informational privacy rights. These problematic provisions will now be analysed in turn.

---

[70] Ibid para 18.
[71] *Bernstein* supra note 60 para 75.
[72] Ibid para 67.
[73] *Hyundai* supra note 26 para 18.
[74] Ibid.
[75] A Roos 'Legal Protection of Personal Information' in J Neethling, JM Potgieter & A Roos *Neethling on Personality Rights* 2 ed (2019) 365.
[76] I Currie 'The Concept of Privacy in the South African Constitution: Reprise' (2008) 2008(3) *TSAR* 549 at 553.
[77] Roos op cit note 75 at 366.
[78] A Roos 'Core principles of data protection law' (2006) 39(1) *CILSA* 102 at 106.

3. LEGISLATIVE DISTINCTION BETWEEN NATURAL AND JURISTIC PERSONS

3.1. POPIA AND NATURAL v JURISTIC PERSONS

The treatment of juristic persons as data subjects is ill-fitted within SA law and, as it will be argued, provides impetus to libertarian legal theory's argument against over-regulation. The Promotion of Access to Information Act[79] and POPIA are corresponding pieces of legislation, as evidenced by the facts that PAIA governs transparency and access to information,[80] POPIA governs the protection of personal information,[81] and that the Information Regulator is a single office dealing with both PAIA[82] and POPIA[83] matters.

Confoundingly, the definitions in these statutes are contradictory. A data subject is defined under POPIA as the natural or juristic person to whom the information which is processed belongs, with personal information being defined to include practically all information which belongs to a natural or juristic person.[84] However, under PAIA personal information does not relate to juristic persons, as PAIA defines personal information as various 'information relating to a natural person'.[85] It is anomalous that personal information applies to natural persons only, under PAIA, and both to natural and juristic persons under POPIA.

Indeed, POPIA's application not only differs from PAIA's application, but it also differs from the GDPR, which, as is the case with PAIA, excludes juristic persons from its definition of personal data (personal information).[86] A major proportion of jurisdictions exclude juristic persons from their definitions of data subjects,[87] with this author agreeing that the reason for such exclusion is that the concept of data protection finds relevance as a legal mechanism to shield natural persons from the (unlawful and/or unwanted) processing of their personal data, and not the processing of a juristic person's data.[88] It has been argued that markets are less unencumbered

[79] 2 of 2000 (hereinafter referred to as PAIA).
[80] Ibid ss 9(*a*), (*c*) and (*e*).
[81] Section 2(a) of POPIA
[82] Sections 32, 83-85 of PAIA.
[83] Section 39 of POPIA.
[84] Ibid s 1.
[85] Ibid.
[86] GDPR, Art. 4(1).
[87] Roos op cit note 78 at 105.
[88] Ibid.

than their counterparts when they adopt free market or libertarian approaches, as these approaches resist the economic over-regulation by governments over property rights.[89] According to Croley, government regulation indisputably imposes transactional, informational and coordination costs,[90] as is the case in respect of SA where it will be argued, inter alia, that POPIA's onerous security requirements and restrictive direct-marketing provisions serve to stifle economic growth, with the corollary being an 'improved state of affairs.[91]

3.2. THE GDPR V POPIA

Save for exclusions found under ss 6 and 7 of POPIA, POPIA is applicable in respect of the processing of a data subject's personal information, with the personal information being entered into a record by or on behalf of a responsible party, regardless of whether automated or non-automated means are used for this purpose, provided that the utilisation of non-automated means are followed by the storage of personal information in a filing system, or an intended filing system, in SA.[92] In contrast to the GDPR, which defines a data subject as an 'identified or identifiable natural person',[93] POPIA provides for the protection of juristic person's personal information. The reason for this distinction may be that the European Convention of Human Rights[94] does not recognise a juristic person's right to privacy.[95] This has been clarified in the case of *Marckx v. Belgium*,[96] which held that Article 8 of the ECHR was drafted to protect a natural person's rights to privacy.[97] Thus, in Europe, juristic persons' rights to privacy are not recognised to the same extent to which such rights are recognised under South African law. This paper propounds that any juristic person's information worth protecting under POPIA is already protected under the common law right to privacy, with intellectual property being historically protected,[98] and rightly so.

It must be noted that POPIA's reference to a juristic person as constituting a data subject – where applicable – is understood to mean a reference to the personal

---

[89] Croley op cite note 30 at 181.
[90] Ibid at 187.
[91] Ibid at 181.
[92] Section 3(1)(*a*) - (*b*) of Act 4 of POPIA.
[93] GDPR, Art. 4(1).
[94] European Convention on Human Rights, as amended (ECHR).
[95] ECHR, Art. 8(1).
[96] IHRL 22 (ECHR 1979) 13th June 1979.
[97] Ibid para 31.
[98] *Sage* supra note 47 at 21.

information of the directors or partners of/within juristic persons.[99] This was not the intention of the Law Commission, which sought the protection of a juristic person's credit information, or information supplied to the state for statistical purposes, and so forth.[100] Additionally, the relevance of extending data-subject protection to juristic persons was for the purposes of protecting the information of sole proprietors (natural person businesses who, when faced with privacy violations, are denied protection of the actio iniuriarum which is afforded to comparable juristic person businesses),[101] corporate strategies, employees' personal information, including special personal information, and so forth.[102] This paper avows that for legislation to protect the details pertaining to company personnel, their position in a corporation and their corporate contact details (i.e. information exclusively related to the corporation itself) would not constitute an appropriate protection of the right to privacy.[103] The personal information of juristic persons which was intended to be protected by POPIA's inclusion of juristic persons as data subjects is akin to the processing of information requiring prior authorisation, such as for the purposes of credit reporting.[104] However, such distinctions are not found under POPIA and it falls foul of over-regulation by failing to clarify the circumstances under which a juristic person is deemed a data subject.

Further, were POPIA to have extended the definition of a data subject to include juristic persons solely for the reason of extending protection of a company's personal information to juristic persons, this would have been achieved by limiting the circumstances under which a juristic person and sole proprietor shall constitute a data subject: when the information in question is of a confidential nature. As such, the legislator neither took heed of the South African Law Commission's Discussion Paper,[105] nor did it borrow from European legislation, notwithstanding the South African legislature's reliance on the European Directive 95/46 (the GDPR's predecessor) in the drafting of POPIA.[106]

---

[99] Y. Burns & A. Burger-Smidt *A Commentary on the Personal Information Act* (2018) 19.
[100] Ibid; see also South African Law Commission Discussion Paper 109 (Project 124) *Privacy and Data Protection* (2005) 10.
[101] Ibid.
[102] Burns op cit note 99 at 19.
[103] *Sage* supra note 47 at 21.
[104] Section 57(1)(*c*) of POPIA.
[105] SALC op cit note 99.
[106] Burns op cit note 99 at 8.

3.3. CONCLUDING REMARKS

From a practical perspective, with juristic persons being included as data subjects under POPIA, free trade will be stifled. Section 2(a)(*ii*) of POPIA hints at the importance of protecting commerce, in the form of the 'free flow of information' as of course, without the free flow of information, businesses would not survive. As Roos states: 'Information is the fuel that drives the economy'[107] Further, s 2(a)(*i*) states that POPIA is relevant in achieving a balance between access to information – which businesses require in order to operate – and the safeguarding of the right to privacy. Instead of merely protecting corporate strategies, and employees' personal information,[108] POPIA is deeming other information belonging to a company (company information), such as contact details, business address, company objectives, and so forth, as protected information.[109] This will, in turn, negatively impact free trade as responsible parties will be burdened if they are required to protect the information of both natural and juristic persons, thereby stifling business growth – especially for small businesses. It is thus recommended that juristic persons are permitted to trade freely, as per libertarian legal theory, and that over-regulation is rejected in favour of the free market approach.

4. SECURITY REQUIREMENTS

4.1. SECURITY REQUIREMENTS UNDER THE GDPR V SECURITY REQUIREMENTS UNDER POPIA

In terms of s 19(1) of POPIA:

> "A responsible party must ensure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent (*a*) loss of, damage to or unauthorised destruction of personal information; and (b) unlawful access to or processing of personal information."

Under art. 31(1) of the GDPR:

---

[107] Roos op cit note 75 at 365.
[108] Burns op cit note 99 at 19.
[109] Section 1 of POPIA sets out that contact details and addresses constitute personal information, which is worthy of protection in respect of natural persons. Where this information belongs to juristic persons, if not intentionally placed the public domain, may not be processed by another natural or juristic person for the purposes conducting business with the juristic person data subject.

> "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity […] for natural persons" [the responsible party is required to implement] "appropriate technical measures to ensure a level of security appropriate to the risk…"

Under the GDPR, the principle of security imposes obligations on responsible parties and operators in order to ensure that data subjects' data are safeguarded.[110] However, the GDPR also acknowledges the costs involved in implementing security measures aimed at protecting natural persons data.[111] Thus, under the GDPR, appropriate technical and organisational measures are examined on a case-by-case basis, and could constitute the use of pseudonyms to protect data subjects' identity, the encryption of personal data, and the conducting of regular tests in assessing the protective measures utilised by responsible parties and operators.[112]

Were POPIA to recognise the relevance of the state-of-the-art and the cost of implementation, in particular, POPIA would not only provide greater clarity to businesses but also shed light on its requirements for responsible parties to take 'appropriate' and 'reasonable' measures — a positive result. However, this cure would be remain insufficient as a business which processes data is required to take steps aimed at protecting data of not only natural persons, but also juristic persons.[113]

Resultantly, it is not inconceivable to imagine that a business which historically operated in both Europe and SA may be more inclined to divest from, and stop operating in, SA were it to operate on a business-to-business ("B-B") scale, i.e., only have clients which are businesses, as opposed to clients which are natural persons. Secondly, foreign businesses which operate in the B-B market may naturally not elect to enter the SA market as POPIA places obligations on these businesses to process juristic persons' data in the same manner the company would process natural persons' data. Additionally, under the GDPR, a responsible party is not required to notify the authorities of a security compromise if it is unlikely (alternatively, unless it is likely) that the compromise will pose a risk to the data subjects' 'rights and freedoms'.[114] This is in direct contrast to POPIA which effectively imposes a blanket requirement on

[110] General Data Protection Regulation, Recital 39 and Art. 5 (1) (f); Modernised Convention 108, Art. 7.
[111] General Data Protection Regulation, Art. 32 (1).
[112] Ibid; see also Council of Europe, European Union Agency for Fundamental Human Rights *Handbook on European data protection law: 2018 Edition* (2018) 165-71.
[113] Section 1 of POPIA.
[114] Council of Europe op cit note 112 at 165.

responsible parties to notify data subjects of data breaches[115] - unlike under the GDPR, the only circumstance under which POPIA does not require a responsible party to notify a data subject is if such notification may impede a criminal investigation on the behalf of authorities.[116] Foreign companies in or entering the SA marketplace would thus subject themselves to more onerous data protection laws in order to operate in SA. The author is of the view that as SA over-regulates informational privacy in that it extends data protection to juristic persons as data subjects, and as this differs from the European regime, this may prove negative to direct foreign investment into SA, for the simple reason that this over-regulation will naturally result in foreign B-B businesses incurring additional transaction, information, co-ordination and legal costs[117] in its expansion of operations into SA, as opposed to an expansion of operations into a jurisdiction which does not impose onerous informational privacy compliance in a B-B market as the author is of the opinion that it has been correctly argued that the balance between privacy and innovation (business) will not be struck through regulation.[118]

4.2. SECURITY REQUIREMENTS AS/AND MARKET-REGULATION

The hurdles placed by POPIA, in front of small businesses and start-ups, result in a sort of market-regulation. First, established businesses with security budgets, or the abilities to accommodate security budgets, will thrive by virtue of smaller businesses' failure to compete with larger businesses. This market-regulation may occur out of fear of smaller companies' receiving fines (or imprisonment of directors), or through the actual receipt of company-crippling fines.

Secondly, data subjects may choose, for the sake of the comfort of knowing that well-established businesses are *capable* of affording to implement appropriate data security safeguards, to conduct business with well-established companies to the exclusion of small businesses and start-ups. Nyoni and Velempini believe that self-regulation (i.e., an absence of privacy laws) will result in the growth of companies

[115] See s 22(1) of POPIA which requires should reasonable grounds exist of a security breach, a responsible party notify the Regulator and the data subject of a breach of data subjects' personal information being held by the responsible party.
[116] Section 22(2) of POPIA.
[117] Croley op cite note 30 at 187.
[118] JE Cohen 'Informational Privacy Litigation as Bellwether for Institutional Change' (2017) 66(2) *DePaul Law Review* 535 at 576.

which adopt and uphold strong privacy policies in a landscape which favours self-regulation and a general absence of privacy legislation.[119]

This author believes that self-regulation, whether complete, or partial – such as through codes of conduct as envisioned under s 60 of POPIA – will result in the growth of companies which *adopt* strong privacy policies. Conversely, POPIA will result in the growth of businesses which have the financial means to adopt and uphold strong privacy measures, regardless of whether the businesses actually implement the required data security measures. This is a classic case of 'perception is reality' as data subjects would likely believe, whether speciously or otherwise, that better-known businesses which can afford to implement security measures, will implement security measures.

Furthermore, through market-regulation, POPIA fails to promote innovation, and for the purposes of this research report, it fails to promote the growth of the SA technological market – ironically both being objectives of ECTA.[120] Juristic persons which are able to afford to implement safeguards will do so, and companies which are unable to (such as start-ups and small businesses) may be fearful of opening up a business without being able to ensure that their clients' data is being protected. POPIA imposes fines on companies for contravening its obligations,[121] and notably does not distinguish between companies on any bases, and particularly not on turnover. However, it cannot be that smaller businesses are not bound by POPIA, as not only would this pose problems to unknowing clients, but it would not be unlikely that persons choose only to conduct business with larger businesses which are able to afford to implement privacy protection measures.

Thus, POPIA has created an environment in which there exists no distinction between self-regulation and market-regulation, at least according to Nyoni and Velempini,[122] as POPIA will act to exasperate, and prevent from entering markets, any business without the means to adopt data security measures, or to be perceived to be able to adopt security measures. From a libertarian perspective, the result will be fewer newer businesses being incorporated, fewer business surviving and fewer people

[119] P Nyoni & M Velempini 'Data protection laws and privacy on Facebook' (2015) 17(1) *South African Journal of Information Management* 1 at 2.
[120] Sections 2(1)(*a*) and 2(1)(*i*) of ECTA.
[121] Sections 107 and 109 of POPIA.
[122] Nyoni op cit note 119 at 2.

being employed – all at the hands of over-regulation. A further issue to the security provisions pertain to ambiguity surrounding the concept of 'reasonableness.

4.3. REASONABLENESS

Section 19(1) of POPIA requires a responsible party to 'secure the integrity and confidentiality' of data subjects' personal information. Section 19(2) qualifies s 19(1) by stating that in securing personal information, a responsible party must take 'appropriate, reasonable technical and organisational measures'. Although Roos is silent on the reasonableness requirement, Roos understands 'appropriate' measures to require the adoption of accepted general, or industry-specific industry measures, including those prescribed by law or regulation.[123] Burns & Burger-Smidt second Roos's understanding of s 19(1).[124] Burns & Burger-Smidt note the Law Reform Commission's reliance on increased credit card theft through hacking[125] as one reason for s the inclusion of 19(1)(*b*) (unlawful access to or processing of personal information).[126]

While the above interpretations are helpful, they fail to account for the negative practical implications on juristic persons. For example, Company A would, through a reading of s 19(1) of POPIA, understand that it 'must' secure personal information of its data subjects – this is instructive. This appears to be an absolute requirement - an excessively high threshold which is, in fact, not appropriate. On the contrary, when reading s 19(2), Company A would be left not knowing whether their responsibility is absolute, or whether they ought to merely act reasonably, as s 19(2) requires that reasonable steps be taken in 'identify[ing] risks' to personal information under their control.[127] This is an untenable situation as the process of identifying risks is akin to securing the 'integrity' of the personal information. Moreover, one cannot be half pregnant - either personal information is, or is not, secure from loss or unapproved destruction,[128] or from being unlawfully accessed.[129] Finally, a responsible party may not take reasonable steps, and successfully secure personal information, or take reasonable steps, yet not successfully secure personal information, thus it is unclear,

[123] Roos op cit note 75 at 388.
[124] Burns op cit note 99 at 71.
[125] SALC op cit note 99 at 66-9.
[126] Burns op cit note 99 at 70.
[127] Section 19(2)(*a*) of POPIA.
[128] Ibid s 19(1)(*a*).
[129] Ibid s 19(1)(*b*).

from a reading of ss 19(1) and (2) of POPIA, whether the security requirements are absolute, or not, and if not, whether the fact that reasonable (or appropriate) steps were taken in securing personal information would be a sufficient defence for the responsible party to avoid liability from a contravention of the provisions of POPIA.

To borrow from, and lend, Jones' quote to the realm of privacy law in a SA context: 'Innovation, though universally coveted and fiercely protected today, has its ups and downs'.[130] Regrettably, South African innovators are potentially experiencing a 'down' at the hands of POPIA, and in particular, due to POPIA's excessive, or otherwise ambiguous, security requirements, which are not, in this author's opinion, appropriate to either to juristic person.

Contrariwise, Swales is of the opinion that the societal benefit of a juristic person's compliance (as a responsible party) with the provisions POPIA – and specifically with condition 6 (openness) – being increased data protection, will outweigh the immediate cost to juristic persons (responsible parties) in conforming with POPIA's requirements.[131] In furtherance of this point, Swales opines that the costs of compliance, while borne by the juristic person, will be passed on to, and felt by, the data subject (consumer).[132] This author disagrees with Swales' assertion that the data subject will foot the bill of a juristic person's compliance with POPIA's security requirements: it appears that Swales has mistaken condition 6 (openness) with condition 7 (security safeguards), as found in s 19 of POPIA as the cost of 'maintain[ing] the documentation of all processing operations'[133] would no doubt constitute a minor cost, when compared to the costs to be reasonably incurred in complying with POPIA's onerous security safeguard requirements. Be that as it may, Swales questions whether responsible parties would be able to avoid passing on the cost of maintaining documentation to the data subject,[134] and is silent on any cost implications on the data subject when discussing condition 7.[135] This author is of the

[130] Jones, M 'Does technology drive law: The dilemma of technological exceptionalism in cyberlaw' (2018) 2018(2) *University of Illinois Journal of Law, Technology & Policy* 249 at 280.
[131] Lee Swales 'Protection of Personal Information: South Africa's answer to the global phenomenon in the context of unsolicited electronic messages (spam)' (2016) 1 *SAMLJ* 49 at 63.
[132] Ibid.
[133] Section 17 of POPIA.
[134] Swales op cit note 134 at 63.
[135] Ibid at 63-4.

view that POPIA's security requirements are unreasonable due to their vagueness, with the result being an over-extension of government and a stifling of the free-market.

Consider how the meaning changes in a different version of s 19(1) were the placement of the word 'reasonable' to be adjusted:

> "A responsible party must implement appropriate, technological and organisational measures to ensure the reasonable security of personal information under its control or possession."

The difference in meaning between the current and proposed versions of s 19(1) is that the current version requires information to be secure (a high threshold), with the words appropriate, technical and organisational being used to qualify how responsible parties may secure personal information. The placement of 'reasonable' in the current version seemingly lowers the threshold as either the steps taken are sufficient or they are not. The current reasonableness requirement is thus seemingly irrelevant; alternatively, it is counter-intuitive. The proposed version attempts to clear up the confusion caused as the threshold of personal information being reasonably secure is a lower threshold, and is in line with the qualifier (s 19(2)), being: appropriate, technological and organisational steps. This interpretation is favoured by the author as, were we to assume that the current meaning of s 19(1)(*a*) of POPIA were to mean that responsible parties *must* (my emphasis) secure personal information, it would pose a risk to innovation and to the ability of small businesses to survive.

In addition to the expenses to be incurred by a responsible party in ensuring compliance with condition 7, its vagueness is a cause for concern as the risks, both internal and external, that are 'reasonably foreseeable' to a responsible party, are subject to debate and will be subject to accepted industry standards at the time of the security breach.[136] There exists an issue as companies of different sizes and financial power would not only would there be a grave difference between the security software and other technological advancements which both different companies could afford, but the hiring power of companies would differ, too. Thus, POPIA should consider the subjective element: a lesser-experienced security officer with fewer resources at his disposal is going to be subject to the same, objective standards as a more-experienced security officer with a wealth of technological resources at his disposal.

[136] Ibid at 63.

Condition 7 practically requires that every company utilise the skillset of an experienced and over-qualified risk or technology officer. This would create a financial burden on all small companies and start-ups. The test would, no doubt, be what a reasonable information technology officer in a market-leading company would believe to constitute a risk, with this belief being substantiated by the fact that appropriate measures ought to be industry-specific, and not company-size-specific.[137] Accordingly, the test would not be what a reasonable technology or risk officer in a small company or start-up would view as a risk. If the latter were the case, which would result in an absurdity, then the law would not apply generally to all data subjects and data subjects are incidentally clients of larger responsible parties would be benefitting from POPIA's protection more so than data subject clients of smaller responsible parties. Perhaps a solution may be for the reasonable foreseeability to be linked to the type of personal information which is processed, albeit still along industry lines,[138] for example a long-term insurance company which processes medical information (special personal information under s 26 of POPIA) should be held to higher security standards than a long-term insurance company which processes information pertaining buy-sell agreements, and thus financial information of the natural person data subject (personal information which is not included as special personal information under s 26).

A further issue with reasonableness is as follows: The s 19(2) measures to be taken by a responsible party includes conducting risk assessments,[139] "establish[ing] and maintain[ing] safeguards" against identified risks,[140] "regularly" ensuring the continuous implementation of the safeguards,[141] and constantly updating safeguards.[142] It must be noted that this author is of the view that under the provisions of POPIA there exists no distinction between 'reasonable' and appropriate – this is seemingly in line with Roos and Burns and Burger-Smidt's understanding of ss 19(1)-(2) of POPIA by virtue of their failure to recognise, or at least note, a distinction between the two concepts.[143] The s 19(2) obligations would no doubt be more onerous

[137] Section 19(3) of POPIA.
[138] Swales op cit note 134 at 63 at 63.
[139] Section 19(2)(*a*) of POPIA.
[140] Ibid s 19(2)(*b*).
[141] Ibid s 19(2)(*c*).
[142] Ibid s 19(2)(*d*).
[143] Roos op cit note 75 at 388; Burns op cit note 100 at 71.

to businesses with lower profits and smaller budgets as s 109(3)(*f*) does not differentiate between companies based on any factors. This is contrary to the delictual principle of negligence where the cost of prevention (affordability) of a harm, should be weighed up against the degree of risk on behalf of an offender, the possible extent of the risk and the role of the offender's conduct.[144]

By way of example, a start-up in the medical insurance industry would process the same categories of personal information as a well-established company in the medical insurance industry. The s 19 obligations on both companies are identical and the fines to be imposed on them under s 109 would not differ either, despite vastly different costs of prevention through the implementation of security measures. This is so as s 19(3) states that a responsible party ought to be apprised of (and surely implement) necessary security requirements relevant to its particular market or industry. Further, s 109(3) (which deals with the factors to be considered by the Information Regulator when quantifying an administrative fine) does not differentiate between responsible parties based on any factors, and notably does not take into consideration the respective companies' size, asset value or turnover. On the contrary, s 109(3)(*f*) appears to impose greater difficulties on smaller companies (by asset value and/or turnover) as the Information Regulator, when quantifying the administrative fine to be imposed on a responsible party, will consider whether the responsible party 'could have prevented the breach from occurring'. Herein lies the issue the standard of reasonableness (or appropriateness). The start-up should be aware of the security requirements required in the insurance industry[145] and thus, with that knowledge, prevent breaches from occurring, if not for financial difficulties. Were 'reasonable' to have been inserted into s 109(3)(*f*) as follows: 'whether the responsible party could have reasonably prevented the contravention from occurring', the Information Regulator would no doubt be prescribed to take into account the financial situation of respective companies, and companies' inability to compete with well-established companies in the same industry, while concurrently respecting the affordability consideration in respect of negligence under delict.

[144] *Mostert v Cape Town City Council* [2000] 4 ALL SA 379 (A) para 35; see also *Ngubane v South African Transport Services* 1991 (1) SA 756 at 776I.
[145] Section 19(3) of POPIA.

4.4. RECOMMENDATION: CALCULATION OF FINES FOR SECURITY BREACHES

In addition to the s 109(3) considerations when imposing a fine, the Regulator should set out, in appropriate regulations, the maximum fines to be imposed on contravening responsible parties.[146] This author avers that (maximum) fines should be determined in accordance with the annual revenue of a responsible party in the preceding twelve months, with an example provided in Table A below.

This concept is borrowed and adapted from the National Credit Act (NCA),[147] Consumer Protection Act (CPA)[148] and Broad-Based Black Economic Empowerment Act[149] which do not apply at all to juristic persons with asset value or annual turnover above a certain threshold,[150] and which applies in limited instances to juristic persons which do not breach the threshold.[151] A final consideration is the method utilised by the South African Revenue Service for taxing natural persons: the greater a natural person earns, the more tax the natural person will pay.[152] Similar to the tax method mentioned immediately above, by fining larger businesses greater amounts, and smaller businesses lesser amounts, for breaches of the provisions of POPIA, the consequence of the breaches would be felt in a more relative fashion by the different-sized businesses. Larger companies have the abilities to pay higher fines and smaller companies would not be fined disproportionately large fines for breaching the provisions of POPIA. Indeed, to fine both the companies which earn revenues of R5 thousand and R50 million in a year, respectively, a fine of R10 million for both breaches of the provisions of POPIA[153] would be incompatible with the object of the economic growth of a country. A further example of this is bail, where one of the considerations in respect of the quantum of bail for an accused is financial means.[154]

---

[146] Section 112(2)(*m*) of POPIA.
[147] National Credit Act 25 of 2002.
[148] Consumer Protection Act 71 of 2008.
[149] Broad-Based Black Economic Empowerment Act 53 of 2003.
[150] See section 4(1)(*a*) of Act 34 of 2005 and section 5(2)(*b*) of Act 71 of 2008; see also s 4(1) of the Statement 000: General Principles and the Generic Scorecard, issued under s 9 of Act 53 of 2003, which exempts companies from application should the companies' annual revenue not exceed the threshold.
[151] Section 6 of the NCA.
[152] SARS 'Rates of Tax for Individuals' available at *https://www.sars.gov.za/tax-rates/income-tax/rates-of-tax-for-individuals/*, accessed on 14 October 2022.
[153] Section 109(2)(*c*) of POPIA.
[154] Section 60(2B)(*a*) of the Criminal Procedure Act 51 of 1997.

A weighted fine-structure would result not only in small businesses not being pushed out of respective markets due to fear on behalf of the data subject that the responsible party's security software is not state-of-the-art, but also in a data subject being able to make educated estimations as to the amount of money invested into data security by the respective service providers, and decide with whom to share personal data on that basis, amongst other factors. A weighted fine structure would promote, and not unduly restrict, trade, with a positive knock-on effect on business and thus employment (freedom of trade).

Table A – Proposed fines for Responsible Parties in contravention with the provisions of POPIA

	Fine for companies with the following annual Turnover of Responsible Party in preceding 12 months		
Section(s) breached	> R1 million	R1 million < > R10 million	> R10 million
107(a) (100, 103(1), 104(2), 105(1), 106(1), 106(3), 106(4))	R100 000.00	R500 000.00	R5 000 000.00
107(b) (59, 101, 102, 103(2), 104(1)	R10 000.00	R50 000.00	R500 000.00
109	R100 000.00	R500 000.00	R5 000 000.00

Having argued that the security requirements under POPIA constitute an over-regulation as they are too stringent, impose unreasonable requirements on juristic persons and through the lack of distinction between different sized companies, will serve to minimize trade, as opposed to support trade, a further issue which requires attention is that of civil liability, and how the civil liability provisions under POPIA will have similar effects on trade as the security provisions.

5. CIVIL CLAIMS UNDER POPIA

5.1. STRICT LIABILITY

"A data subject [..] may institute a civil action for damages […] against a responsible party […] whether or not there is intent or negligence on the part of the responsible

party."[155] POPIA's provisions result in a situation in which small companies and start-ups will either be further burdened by an interpretation of POPIA to impose strict liability, or they may be disinclined to conduct business in SA due to a lack of clarity surrounding the relationship between POPIA's and strict liability. One school of thought believes that POPIA imposes strict liability on infringers, as fault, a requirement for a common law privacy action,[156] is seemingly not a requirement under s 99(1) of POPIA, with s 99 governing the civil remedies available to a data subject whose POPIA rights have been infringed. The argument is as follows: a data subject will be entitled to institute a claim for civil damages against a responsible party without the responsible party being at fault for the infringement as the wording of s 99(1) provides that a data subject (including the Information Regulator on the data subject's behalf) may 'institute a civil action for damages' against a responsible party who has contravened numerous provisions of POPIA, regardless of whether the responsible party acted negligently or intentionally.[157] Depending on the correct interpretation of s 19(1) of POPIA, the argument of strict liability may be further strengthened should s 19(1) be read to impose strict liability on responsible parties, which 'must secure' the safekeeping of personal information under their control, by using appropriate, reasonable, technological and organisation measures, in order to refrain from having personal information lost, damaged, destroyed without authorisation, or accessed unlawfully.[158] This rationale is untenable, however, and ought to be formally debunked expeditiously as the dangers of such a school of thought compounds the growing number of issues identified for companies without financial means to implement sufficient data security measures to participate in the South African economy.

The first counter-argument presented against the premise that POPIA imposes strict liability on data subjects lies in an analysis of s 109(3). It cannot be that strict liability applies in respect of civil proceedings but not in terms of administrative fines imposed by the Information Regulator. Section 109 fines apply in respect of any alleged offence of the provisions of POPIA. It may be argued that an interference, as referred to under s 73 of POPIA, and being a requirement for a s 99 civil claim, is

[155] Section 99(1) of POPIA.
[156] *Jansen van Vuuren v Kruger* 1993 (4) SA 842 (AD) at 36.
[157] D Millard and EG Bascerano 'Employers' Statutory Vicarious Liability in Terms of the Protection of Personal Information Act' (2016) 19 *PER / PELJ* 1 at 23.
[158] Section 19(1)(*a*) of POPIA.

different from an offence (and thus the counter-argument would be rejected). However, it appears that this is not the case as the Information Regulator is required, in quantifying the administrative fines to be imposed on a responsible party who has committed an offence under POPIA, to consider: the extent of the data subjects impacted by the 'contravention';[159] the probability of a data subject suffering damages from the contravention;[160] the possibility of the responsible party having avoided the contravention;[161] and the failure of the responsible party to conduct risk assessments.[162] Not only does s 109(1) refer to offences (which are referenced under s 107 and have limited application), but s 109(3) also refers to contraventions and offences of the provisions of POPIA, with contraventions referring both to offences (as per s 107) and breaches (as per s 99). Moreover, s 109(3)(*g*) concerns the conducting of risk assessments – a requirement under s 19(1) of POPIA.

POPIA's utilisation of strict liability is problematic as strict liability is not required in respect of common law privacy claims (civil claims);[163] however, liability is an absolute requirement in terms of certain crimes requiring intent – meaning that strict liability is not permitted in criminal cases, and is actually unconstitutional.[164] Hence, POPIA has effectively inserted the application of strict liability under South African law. The purpose of strict liability is that victims may receive compensation from perpetrators 'at low cost' and that perpetrators 'do not benefit at the victims' expense',[165] or, to protect many at the hands of a few, which concept is criticised by Nozick in his rejection of governments imposing higher taxes on the wealthy.[166] Nozick, as does libertarianism, supports an individual taking responsibility for one's own actions, as opposed to regulations dictating one's actions, which is evidenced from Nozick's term of "side constraints" – an individual's responsibility to take responsibility over one's own actions and to ensure that one's actions do not infringe

[159] Section 109(3)(*c*) of POPIA.
[160] Section 109(3)(*e*) of POPIA.
[161] Section 109(3)(*f*) of POPIA.
[162] Section 109(3)(*g*) of POPIA.
[163] David Mcquoid-Mason 'Invasion of Privacy: Common law v Constitutional Delict – Does it Make a Difference? 2000 *Acta Juridica* 227 at 229.
[164] *S v Masingili and others* 2013 (2) SACR 67 (WCC) para 5.
[165] Gerald P. O'Driscoll 'Pollution, Libertarianism, and the Law' (1982) 2 *Cato Journal* 2(1) 45 at 46.
[166] Adrienne E van Blerk *JURISPRUDENCE An Introduction* (1998) 137.

on the rights of others.[167] Thus, strict liability is the contrary to the libertarianism legal project as it comprises over-regulation and it rejects the individual responsibility.

Additionally, other sections under POPIA reject the notion of strict liability under POPIA. For the purposes of this argument, s 12(2)(*b*) shall be explored. It permits a responsible party (Company C) to collect a data subject's personal information from a third party (Company D) were the data subject to have provided Company D with consent to indirect collection. Of course, Company C would not have received consent directly from the data subject, and would have relied on Company D's representations. Assuming that Company C was not aware of the misrepresentation and was not acting maliciously, were Company D to have constructed the data subject's consent, Company C would not necessarily have been negligent in its indirect collection of personal information. Should s 99(1) impose strict liability on responsible parties, Company C would be liable to the data subject for Company C's indirect collection of the data subject's personal information, notwithstanding that Company C's contravention of s 12 of POPIA was neither negligent nor intentional. Therefore, it appears that the legislature's lack of concern for whether a responsible party which has contravened one of the sections referred to in s 73 of POPIA, acted with negligence or intent, is merely a method of the legislature stating that no action for a breach of the provisions of POPIA may automatically be precluded. Whether a responsible party breached POPIA through an act of negligence or intent, a data subject may not be precluded from accessing court to enforce its rights - as provided for under s 34 of the Constitution.

Nonetheless, the potential consequences of confusion caused by the drafting of s 99(1) is unpalatable to the author. Should responsible parties not reject the strict liability argument, it would result in the stifling of innovation and economic growth due to a fear of POPIA imposing strict liability on the responsible without the means to abide by POPIA's conditions, beyond reproach. Additionally, should data subjects not adopt this school of thought, the result may be that companies view their participation in specific industries as not worth the risk as s 99 may be viewed as an invitation for disgruntled data subjects to utilise s 99 remedies with alacrity. Therefore, the author proposes that s 99(1) be amended, in curing the confusion caused by it, to omit the

[167] Ibid.

reference to 'intent' and 'negligence', for strict liability is in direct contrast with libertarianism, as has been argued above, and thus the freedom of trade.

5.2. VICARIOUS LIABILITY

For the purposes of the right to privacy, the common law concept of liability concerns a responsible party causing damage or injury to a data subject through an intentional or negligent action, or failure thereof, save for instances of vicarious liability: a scenario in which an employee of a responsible party, or third party related to a responsible party, may be held personally liable for the damage or injury caused to the specific responsible party's data subject.[168] Botha and Millard submit that the test for vicarious liability is two-fold: objective and subjective.[169] An instruction not to perform an action limits the scope of employment and such actions, if committed, would not fall under the scope of employment.[170] The subjective frame of mind of the employee and the objective relationship between the employee and employer's interests would be investigated to determine whether infringing actions were performed under the scope of employment.[171] However, the absence of a defence against vicarious liability under POPIA, as will be investigated below, would entail that an employer is almost completely precluded from escaping liability for its employee's contravention of POPIA.[172]

In terms of vicarious liability, the data subject need not prove that the employee or third party's breach of the provisions of POPIA is wilful or intentional.[173] The common law position is that, both the responsible party and/or the employee and the third party would be liable for the breach.[174] Roos, and Millard and Bascerano Bascerano) criticise POPIA for imposing strict liability on responsible party employers,[175] with vicarious liability being evident by the reading of s 99(1) and supported by the strict liability proponents, as discussed above. This author agrees with Millard and Bascerano that the defences available to responsible party employers

[168] Millard and Bascerano op cit note 157 at 15-6.
[169] Monray Marsellus Botha and Daleen Millard 'The past, present and future of vicarious liability in South Africa' (2012) *De Jure* 225 at 232.
[170] *Bezuidenhout v Eskom* 2003 (3) SA 83 (SCA).
[171] R Le Roux 'Vicarious Liability: revisiting an old acquaintance (2003) 24 *ILJ* 1879.
[172] Millard and Bascerano op cit note 157 at 4.
[173] Ibid at 16.
[174] BE Loots 'Sexual harassment and vicarious liability: a warning to political parties' (2008) 1 *Stell LR* 143 at 151.
[175] A Roos op cit note 75 at 410.

under POPIA are insufficient[176] in that no provision is made for the defence against a claim for vicarious liability. In complete contrast to s 60 of the Employment Equity Act,[177] which governs vicarious liability of employers, and particularly s 60(4) of the EEA, which sets out the requirements to be met by an employer to escape vicarious liability, POPIA contains no such provisions which may come to the rescue of employers for the intentional or negligent breaches of POPIA by the responsible party's infringing employee.[178]

Thus, a responsible party employer, despite taking reasonable steps in line with s 19(1) of POPIA, or otherwise to prevent a breach of POPIA, will nonetheless be held vicariously liable for the fault of its employee or a third party, without the ability of providing a defence as provided for under s 60(4) of the EEA or the common law defence that there was an insufficient nexus between the employee's actions and the purpose of the business of the employer.[179] This is more onerous than the EEA and could result in a diligent company being held liable under a s 99 claim of an administrative fine, for conduct committed by its employee outside the scope of business, and which is insufficiently related for the business of the employer. Indeed, the absence of a defence against vicarious liability may likely result in the stifling of innovation as it would be far safer, from a financial perspective, to breach a provision of POPIA as an employee than as a responsible party employer with a responsible party employer being denied the ability to defend a claim of vicarious liability. Furthermore, to add to the already-high costs required to comply with POPIA's information security requirements, companies would require comprehensive business insurance to cover POPIA claims as there is infringing responsible parties are denied defences against vicarious liability claims.[180]

5.3. DEFENCES

Section 99(2) of POPIA provides for defences which responsible parties may raise against s 99(1) claims brought against them. Section 99(2)(*c*) of POPIA affords a responsible party a defence on the grounds that the data subject was at fault. Fault is

[176] Millard and Bascerano op cit note 157 at 4.
[177] 55 of 1998 (hereinafter referred to as the 'EEA').
[178] Millard and Bascerano op cit note 157 at 4.
[179] K v *Minister of Safety and Security* 2005 (6) SA 419 (CC) para 48.
[180] Millard and Bascerano op cit note 157 at 31.

ordinarily considered when determining an apportionment of damages;[181] however, POPIA has misappropriated the concept of fault. Fault is used as a factor in a damages' equation and is not a defence, something which, if proven, will prove entirely dispositive of the data subject's claim. Furthermore, s 99(1)(*c*) merely states as a defence: 'fault on the part of the [data subject]'. This will have the practical effect of entirely disposing of a data subject's claim, should the data subject be even marginally responsible for the breach of the provisions of POPIA, regardless of the degree of fault on the data subject's behalf. This inclusion would defeat otherwise justifiable claims brought by data subjects based on mere technicalities or otherwise negligible actions on the behalf of the data subject. This will indirectly have the result of stifling the economic growth of small and start-up businesses for, it would not be unreasonable to presume, data subjects would elect to contract with responsible parties with companies with strong reputations – larger businesses – in order to mitigate the risk of a responsible party breaching the provisions of POPIA and a data subject being denied legal recourse by virtue of even the most negligible element of fault on the data subject's behalf. Therefore, it would be preferable to replace s 99(2)(*c*) with the following: 'the factors found under s 109(3) below'. This would align the criminal and civil elements of POPIA and would provide greater clarity to data subjects and responsible parties alike.

5.4. AGGRAVATED DAMAGES

In addition to the awarding of patrimonial and non-patrimonial damages under s 99(3)(*a*) of POPIA, s 99(3)(*b*) entitles a court to award aggravated damages to a data subject under a s 99(1) civil action. Aggravated damages is a foreign concept to SA and to aid the understanding of this concept it is necessary to investigate foreign jurisdictions.[182] Beever notes that the distinguishing factor required to bring about a claim for aggravated damages, as opposed to a claim for punitive damages and damages for mental distress, is the requirement for an affront on the plaintiff's 'moral dignity'.[183] Murphy notes that the type of loss or damages experienced may differ, despite the damage-causing action which caused the loss remaining the same. Correlatively, he points out that even a dog can discern between accidental and

[181] Section 1(1)(*a*) of the Apportionment of Damages Act 34 of 1956.
[182] Sections 39(1)-(2) of the Constitution.
[183] A Beever 'The Structure of Aggravated and Exemplary Damages' (2003) 23 *OJLS* 87 at 89.

intentional harm. Where a defendant intentionally causes harm, aggravated damages are an appropriate form of redress and are utilised to compensate an affront to the plaintiff's dignity—which is only caused through intent and malice; where the defendant lacked intent to cause harm and malice, a claim for aggravated damages would arise.[184] Summarily, aggravated damages are not concerned with outcomes, but rather whether and to what extent the defendant's mental state and malice contributed towards the plaintiff's suffering. According to Murphy, a mere denial of a human right, albeit a denial which is lacking in intention and malice, would not necessarily equate to an attack on one's dignity.[185]

Such issues would be better dealt in terms of delictual claims for self-worth under the actio iniuriarum. Nonetheless, a lack of clarity, due to an absence of s 99(3) case law, poses yet another consideration for small business and start-ups in favour of not continuing with, or commencing, business operations in South Africa. Hence, in order to protect commerce, and the right to freedom of trade, aggravated damages should be removed from s 99(3)(*b*) of POPIA.

6. CONCLUSION

POPIA exposes the issues of the seeming failure of freedom of trade, as found under s 22 of the Constitution, to apply to juristic persons. However, notwithstanding the lack of application of freedom of trade to juristic persons, POPIA's provisions provide impetus to the libertarian rejection of over-regulation. This is so as by POPIA applying the definition of a data subject to a juristic person, business will be stifled as attempting to conduct business with another company, an exercise which should be seamless, will result in myriad potential ways to contravene the law. Furthermore, POPIA's stringent data security requirements will flush out smaller companies and start-ups out of fear of companies receiving disproportionate fines for non-compliance with the provisions of POPIA, or through market-regulation at the behest of consumers. Finally, the confusion surrounding liability, the potential imposition of strict liability, an absence of a defence against vicarious liability and the sudden inclusion of a misplaced

[184] John Murphy 'The Nature and Domain of Aggravated Damages' (2010) 69 *Cambridge Law Journal* 353 at 359.
[185] Ibid at 362.

aggravated damages under POPIA, will result in adverse economic affects, and will stifle economic growth by shutting down, or reducing the size of, businesses in SA.

BIBLIOGRAPHY

BOOKS, JOURNAL ARTICLES AND INTERNET SOURCES

Abdulrauf L and Fombad C 'The African Union's data protection Convention 2014: a possible cause for celebration of human rights in Africa?' (2016) 8 *Journal of Media Law* 67

Albertyn C & Goldblatt B 'Equality' in Stuart Woolman et al (eds) *Constitutional Law of South Africa* 2 ed (Service 12-03)

Allan T *Constitutional Justice: A liberal theory of the rule of law* (2001) Oxford: Oxford University Press

Beever A 'The Structure of Aggravated and Exemplary Damages' (2003) 23 *OJLS* 87

Botha M and Millard D 'The past, present and future of vicarious liability in South Africa' (2012) *De Jure* 225

Burns Y & Burger-Smidt A *A Commentary on the Personal Information Act* (2018) Johannesburg: Lexis Nexis SA.

Cohen J 'Informational Privacy Litigation as Bellwether for Institutional Change' (2017) 66(2) *DePaul Law Review* 535

Council of Europe, European Union Agency for Fundamental Human Rights *Handbook on European data protection law: 2018 Edition* (2018) Luxembourg: Publications Office of the European Union

Croley S 'Libertarianism as Critical Theory' (1996) 1 *Michigan Law and Policy Review 179*

Currie I 'The Concept of Privacy in the South African Constitution: Reprise' (2008) 2008(3) *TSAR* 549

Davis D 'Freedom of Trade, Occupation and Profession' in Stuart Woolman et al (eds) *Constitutional Law of South Africa* 2 ed (Service 12-03)

Hospers J 'Libertarianism and legal paternalism' (1980) 4(3) *Journal of Libertarian Studies* 261

Le Roux R 'Vicarious Liability: revisiting an old acquaintance (2003) 24 *ILJ* 1879

Loots B 'Sexual harassment and vicarious liability: a warning to political parties' (2008) 1 *Stell LR* 143

Mcquoid-Mason D 'Invasion of Privacy: Common law v Constitutional Delict – Does it Make a Difference?' 2000 *Acta Juridica* 227

Millard D and Bascerano E 'Employers' Statutory Vicarious Liability in Terms of the Protection of Personal Information Act' (2016) 19 *PELJ* 1

Murphy J 'The Nature and Domain of Aggravated Damages' (2010) 69 *Cambridge Law Journal* 353

Neethling J 'Features of the Protection of Personal Information Bill, 2009 and the Law of Delict' (2012) 75(2) *THRHR* 241

Neethling J 'The concept of Privacy in South African Law' (2005) 122 *SALJ* 18

Nyoni P & Velempini M 'Data protection laws and privacy on Facebook' (2015) 17(1) *South African Journal of Information Management* 1

O'Driscoll G 'Pollution, Libertarianism, and the Law' (1982) 2 *Cato Journal* 2(1) 45

Papadopoulos S & Tladi S 'Consumer protection in e-commerce' in Sylvia Papadopoulos & Sizwe Snail ka Mtuze (eds) *Cyberlaw @ SA* the law of internet in South Africa 4 ed (2022) Braamfontein: Van Schaik Publishers

Pistorius T & Tada S 'The Hall of Shame – Double Standards for Spam' (2014) 26 *South African Mercantile Law Journal* 688

Roos A *Core Principles of Data Protection Law* (2006) 39(1) *CILSA* 102

Roos A 'Legal Protection of Personal Information' in J Neethling, JM Potgieter & A Roos *Neethling on Personality Rights* vol III 2 ed (2019) Pretoria: Lexis Nexis SA

Roos A 'Privacy in the Facebook Era: A South African Legal Perspective' 129 *SALJ* 375

SARS 'Rates of Tax for Individuals' *available at https://www.sars.gov.za/tax-rates/income-tax/rates-of-tax-for-individuals/,* accessed on 14 October 2022.

Sartori G 'Liberty and Law' (1976) 5 *Institute for Humane Studies* 8

Swales L 'Protection of Personal Information: South Africa's answer to the global phenomenon in the context of unsolicited electronic messages (spam)' (2016) 1 *SAMLJ* 49

Van Blerk A *Jurisprudence: An Introduction* (1998) Durban: Lexis Nexis SA

Van Staden M 'Spontaneous Order or Central Planning? A brief overview of the Libertarian Approach to Law' (2021) 84 *THRHR* 53

CASE LAW

South Africa

Bernstein v Bester NO 1996 (2) SA 751

Bezuidenhout v Eskom 2003 (3) SA 83 (SCA)

Contract Employment Contractors (Pty) Ltd v Motor Industry Bargaining Council (MIBCO) and Others 2013 (3) SA 308 (LC)

De Reuck v Director of Public Prosecutions Witwatersrand Local Division and Others 2004 (1) SA 406 (CC)

Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others 2001 (1) SA 545 (CC)

Islamic Unity Convention v Independent Broadcasting Authority 2002 (4) SA 294 (CC)

Jansen van Vuuren v Kruger 1993 (4) SA 842 (AD)

JR 1013 Investments CC and Others v Minister of Safety and Security and Others 1997 (7) BCLR 950 (E)

K v Minister of Safety and Security 2005 (6) SA 419 (CC)

Mostert v Cape Town City Council [2000] 4 All SA 379 (A)

Minister of Trade and Industry & Another v Murendi Properties and Building Supplies (Pty) Ltd [2021] ZASCA 53

Mukaddam v Pioneer Foods (Pty) Ltd and Others 2013 (2) SA 254 (SCA)

Mukaddam v Pioneer Foods (Pty) Ltd and Others 2013 (5) SA 89 (CC)

Ngubane v South African Transport Services 1991 (1) SA 756 (A)

NM & others v Smith & others 2007 (5) SA 520 (CC)

S v Masingili and others 2013 (2) SACR 67 (WCC)

S v Mhlungu and Others 1995 (3) SA 867 (CC)

Sage Holdings Limited v Financial Mail (Pty) Limited 1993 (2) SA 451 (AD)

Van Rensburg v South African Post Office Ltd 1998 (10) BCLR 1307 (E)

Other jurisdictions

Marckx v. Belgium IHRL 22 (ECHR 1979) 13th June 1979.

LEGISLATION, CONSTITUTIONS, CONVENTIONS AND CODES

South Africa

Broad-Based Black Economic Empowerment Act 53 of 2003

Constitution of the Republic of South Africa, 1996

Consumer Protection Act 68 of 2008

Electronic Communications and Transactions Act 25 of 2002

National Credit Act 34 of 2005

Proc R21 of 2020

Proc R25 of 2014

Promotion of Access to Information Act 2 of 2000

Protection of Personal Information Act 4 of 2013

South African Law Commission Discussion Paper 109 (Project 124) *Privacy and Data Protection* (2005)

Other Jurisdictions

European Convention on Human Rights, as amended (ECHR)

EU General Data Protection Regulation (EU) 2016/679