BEYOND THE CLICK: INFORMED CONSENT IN THE AGE OF COOKIES

by

Student Number: 2499643

Name: Mokone Finger

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.

Supervisor: Dr C Visser

Date: **8 October 2024**

DECLARATION

I, 2499643, declare that this Research Report is my own unaided work. It is 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. It has not been submitted before for any degree or examination in this or any other university.

I have submitted my final Research Report through Turnitin and have attached the report to my submission.

Student Number: 2499643

Word count: 9735

ABSTRACT

Rapid evolution of technology and the internet has enabled vast data to be exchanged amongst people. These changes have introduced extraordinary data collecting methods that also recognise traces of personal information when users browse the internet. An example of such a tracking method is a cookie. Cookies, while they serve to enhance user experience, tend to collect and store personal information of data subjects without their knowledge and consent. For this reason, they raise a question of a threat to privacy and consent of data subjects.

This research report principally examines the legal sufficiency of a mere click of a button in establishing valid consent for processing of personal information, which includes the collection, storage and transmission of personal information through cookies.

The Protection of Personal Information Act 4 of 2013 (the POPI Act) was enacted to give effect to the constitutional right to privacy. Thus, the POPI Act operationalises the constitutional right to privacy by providing a framework for the processing of personal information, even though its application has shortcomings related to consent and cookies. In order to interpret the POPI Act, this paper will integrate the common law and the General Data Protection Regulation 2016/679, based on the adjudicative subsidiarity doctrine, as constitutional backdrop instruments to determine the threshold for consent in the POPI Act when using cookies.

TABLE OF CONTENTS

1. Introduction……..2
2. Theoretical Underpinnings: Integrated Reading Approach……..6
3. Data Protection in South Africa…….9
    a. Introduction and overview of the Protection of Personal Information Act……..9
    b. Definition and fundamental concepts…….10
    c. The POPI Act and Cookies: An Analysis of Consent……...13
4. Common Law Consent……15
5. Cookies and The European Union's General Data Protection Regulation (GDPR)……20
    a. General overview of the GDPR……21
    b. Definitions and fundamental concepts……21
    c. Analysis of Consent……...22
6. Findings and Recommendations……28
7. Conclusion……...33

I INTRODUCTION

In today's digital age, digital footprints have become just as significant as physical ones.[1] As a result, cookies have emerged as a crucial component of the online experience, playing a vital role in the technology countless individuals utilise.[2] On the other hand, research involving consumers familiar with online shopping has found that using cookies can erode trust in a website, reduce the likelihood of repeat business and positive recommendations, and decrease willingness to share personal information.[3]

There is a considerable risk to privacy when personal information is collected from another source under the guise of a consent granted by a click of a button or from another source, such as another website, as is the case for third-party cookies.[4]

The risk in the use of cookies relates to the question of whether individuals are able to decide what information they want to reveal to the public. The collection and storage of information requires the consent of a user; where information is collected without knowledge of a user 'consent under these circumstances is no more than a fiction'.[5]

Thus, what exactly is a cookie? In the context of Information Technology, a cookie is essentially a text file that gets downloaded onto a user's device whenever they visit a website.[6] In practical terms, the website recognises the user's device and stores data generated from the user's interaction with the website.[7] Cookies can store a wide range of information derived from a user's interaction with a website. For

---

[1] S.D.R.M. Weerasinghe Paper on Cookies, Privacy and Cyber Security, University of Moratuwa Sri Lanka 1.
[2] Ibid.
[3] Carolina Curto Silva *Consumer evaluation of cookies for marketing purposes: Case Study of Portuguese Consumers* (Master's degree in Information Management dissertation, Universidade Nova de Lisboa, 2021) 7.
[4] The ICO 'Guidance on the Use of Cookies and Similar Technologies' available at *https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-cookies-and-similar-technologies/#cookies1,* accessed on 25 February 2024.
[5] Firoz Cachalia and Jonathan Klaaren 'Towards a Public Law Perspective on the Constitutional Law of Privacy in South Africa in the Age of Digitalization' (2023) *Journal of African Law* at 11.
[6] Bernard Hamann and Sylvia Papadopoulos 'Direct marketing and spam via electronic communications: An analysis of the regulatory framework in South Africa' (2014) *De Jure* 46. Ebersohn "Internet law: cookies, traffic data and direct advertising practices" (2004) *SAMLJ* 741, 742.
[7] De Stadler et al *Overthinking the Protection of Personal Information Act: The last book you will ever need* (2021) 296.

instance, cookies can store information such as login codes, passwords, credit card details and shopping cart items.[8]

There are different types of cookies .[9] For the ensuing discussion, this paper only aims to discuss third-party cookies.[10] The chief reason for the focus on this type of cookies is that they are more susceptible to exposing vulnerable information to other individuals or software systems. For this reason, in 2002, the European Union published a directive that required website owners to obtain consent of users to this type of cookies when using a website.[11]

Third-party cookies are stored on the website by a third party.[12] These cookies send data subject's information to another website or social media network such as Facebook, usually for marketing purposes.[13] The third party will then send 'targeted' advertisements to the website user.[14] These cookies save significant user information, including the user's online activities, preferences, and location.[15] This information

---

[8] Yvonne Burns & Ahmore Burger-Smit *Protection of Personal Information Law and Practice* 2 ed (2023) 541.

[9] There are two types of cookies, (i) Authentication Cookies which save a user's information, such as a username and password. These cookies create a unique identifier that saves a user's information by allowing a user to access a website at a later stage without having to input the information again; (ii) Tracking Cookies save personalised information of a user, such as personalised searches. These cookies are commonly used by advertisers. See Microsoft 'Everything you need to know about Internet cookies', available at *https://www.microsoft.com/en-us/edge/learning-center/what-are-cookies?form=MA13I2,* accessed on 17 March 2024.

[10] It is important to note that there are two other types of cookies, i.e. First party cookies are composed of a tracker that is generated and stored by the website the individual is currently browsing. The lifespan of first party cookies is temporary and will remain as long as the user is logged on the website, as they are deleted when the data subject completes a browsing session. Given that they do not send information to other website, this type of cookie uses significantly less user information and terminate upon closure of a session. However, lifespan of first-party cookies can vary depending on the website's configuration. Some first-party cookies may have longer expiration dates which can pose risk of threat to privacy. With regard to second party cookies, De Stadler et al rejects that this type of cookie exists as second party is referred to as the data subject and information provided by data subject is referred to as "zero-party data". This refers to information that is disclosed intentionally and proactively by the internet user in order to afford the data processor insight to curate a personalised browsing experience. See De Stadler et al *Overthinking the Protection of Personal Information Act: The last book you will ever need* (2021) 297. See also Paul Herman 'The Cookiepocalypse: Why first-party data is going to matter to your newsroom' available at *https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2022-09/RISJ%20Paper_Paul%20H_TT22_Final_1.pdf,* accessed on 13 February 2024. See further Masha Komnenic 'First-Party vs. Third-Party Cookies: The Differences Explained' available at *https://termly.io/resources/articles/first-party-cookies-vs-third-party-cookies/,* accessed on 13 February 2024.

[11] Microsoft 'Everything you need to know about Internet cookies', available at *https://www.microsoft.com/en-us/edge/learning-center/what-are-cookies?form=MA13I2,* accessed on 24 February 2024.

[12] De Stadler et al *Overthinking the Protection of Personal Information Act: The last book you will ever need* op cit note 7 at 297.

[13] Ibid.

[14] Ibid.

[15] Ibid at 298.

allows the website to track a user's activity across different websites.[16] The chief risk in the use of cookies is in traces that are left behind, when paired with unique identifiers and other information collected through interaction with servers, which can be used to establish a profile and identify a natural person,[17] and resultantly expose their private details.

As articulated earlier, owners of websites that use third-party cookies need the consent of a website user. Websites that use first or third-party cookies often use a tracking wall (also known as cookies walls or cookie notices) that requires users to agree or disagree with all cookies and trackers to use a website.[18]

Practically, cookie notices are seen when a user logs on a website.[19] In most instances, upon accessing a website, users are presented with a consent notice, prompting them to either accept or decline the collection of cookies.[20] In certain cases, the provision of a website's service or functionality is contingent upon obtaining user consent, via a cookie notice, for the storage of information or access to previously stored information on the user's server. Consequently, the legitimacy of the user's consent in such instances may be legally questionable.[21] Where cookie notices do not disclose reasons for harvesting a user's information, such a user may argue that collection of information intrudes on self-determination or autonomy. Website owners are required to disclose the specific nature of the information being collected and the particular cookies used in the process, at a minimum through using cookie notices, to mitigate the deficiencies stemming from a lack of transparency in data collection practices.[22]

While cookies enhance user experience, they also raise critical questions about privacy and consent given the right to privacy as guaranteed in the Constitution. This

---

[16] Ibid at 297.
[17] Van Der Merwe D, Roos A, Pistorious T, Eiselen S and Nel S (eds) *Information and Communication Technology Law* 2nd ed (2016) 364.
[18] CookiePro Knowledgebase 'What is a cookie?', available at *https://www.cookiepro.com/knowledge/cookie-wall/#:~:text=Essentially%2C%20a%20cookie%20wall%20is%20a%20variation%20of,a%20cookie%20wall%20is%20a%20notice-only%20banner%20below,* accessed on 24 February 2021.
[19] Michalsons 'Cookie law in South Africa', available at *https://www.michalsons.com/blog/cookie-law-south-africa/15264*, accessed on 8 October 2023.
[20] Ibid. See Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679 WP259 rev.1.1 (4 May 2020) at 12.
[21] Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679 WP259 rev.1.1 (4 May 2020) at 16.
[22] De Stadler et al *Overthinking the Protection of Personal Information Act: The last book you will ever need* op cit note 7 at 302.

research report principally examines the legal sufficiency of a mere click of a button in establishing valid consent for collecting and processing data through cookies.

This research report aims to determine whether our law prescribes sufficient jurisprudence for requirement or quality of consent to pass legal muster. It is foreseeable that a question relating to the constitutional right to privacy and the Protection of Personal Information Act No. 4 of 2013 (the POPI Act) will arise.

Section 1 of the POPI Act defines "consent", but it does not have provisions specifically dedicated to explaining how it ought to be understood. The POPI Act also references consent in several sections in the Act.[23] When statutory provisions (such as the POPI Act) do not provide clear guidance, Cachalia and Klaaren argue that s 14 of the Constitution will continue to play a central role in how South Africa's privacy law develops in reaction to technological advancements.[24]

This research paper seeks to integrate various sources of law to interpret the requirements for consent when personal information is collected using cookies.

The outline of the paper is set out below to address the aims of the research report.

In section two, I will focus on the theoretical framework based on a single system of law (as predicated by doctrine of adjudicative subsidiarity) to provide an integrated and constitutional reading of different sources of law that apply to consent. This analysis will include an outline of informational privacy.

In section three, I analyse the POPI Act; in particular, I assess the scope of conditions for lawful processing of personal information and analyse provisions related to consent and the relationship with cookies.

In section four, I focus on common law consent in terms of the maxim of *volenti non fit iniuria* as developed by case law in the context of the common law of personality and constitutional development in light of human dignity.

Thereafter, in section five, I will explore the European Union's (EU) provisions of the General Data Protection Regulation 2016/679 (GDPR). The EU has had established data protection laws for a longer period and as a result case law has been

[23] Sections 11(1), 12(2), 14(1), 14(7), 15(3), 18(4), 27(1), 69(1), 72(1) and 106(1) of the POPI Act.
[24] Firoz Cachalia and Jonathan Klaaren op cit note 5 at 11.

tested against it. The drafters of the POPI Act have consulted these instruments and for this reason, the GDPR is useful in interpreting the POPI Act.[25] Even though the GDPR is non-binding in South Africa, a comparative analysis between the POPI Act and the GDPR can offer valuable insights into potential areas for reform in South African law.

Further, in section six, I will consolidate the various sources of law in attempting to answer the critical questions raised in this research report based on an integrated reading strategy (even though I do not discuss the framework in great detail in this paper). Finally, in section seven, I provide a conclusion based on the findings.

II THEORETICAL UNDERPINNINGS: INTEGRATED READING APPROACH

Following the abolishment of parliamentary sovereignty, constitutional supremacy was founded on the basis of the Constitution.[26] Constitutional supremacy is concerned with the promotion of constitutional values of the Constitution when all law is interpreted and developed.[27] Zitzke suggests that constitutional transformation comprising a single system of law can be achieved if all law 'sing the same song (albeit sometimes in harmony and not in a monotone manner'.[28] He posits that an integrated reading strategy called adjudicative subsidiarity that was adopted by the Constitutional Court would help realise the transformative paradigm.[29] The doctrine of adjudicative subsidiarity provides a coherent, integrated reading strategy of the different sources that ensures that transformative constitutional objectives are met.[30]

Visser notes that a single-system of law principle within the law of personality is guided by multiple sources of law emanating from non-constitutional sources of law which are assessed against constitutional control in order to give effect to the constitutionalism transformation.[31]

---

[25] Freedman W and Schultz H 'Plugins and POPI: A Critical Discussion into the Legal Implications of Social Plugins and the Protection of Personal Information' (2023) *PER/PELJ* 18.
[26] Firoz Cachalia and Jonathan Klaaren op cit note 5 at 11.
[27] L Hawthorne 'Legal tradition and the transformation of orthodox contract theory: The movement from formalism to realism' (2006) *Fundamina* 83.
[28] E Zitzke 'Constitutional heedlessness and ever-excitement in the common law of delict's development' (2015) 7 *Constitutional Court Review* 270.
[29] Ibid at 285.
[30] Ibid at 259 and CJ Visser 'Adjudicative subsidiarity, the "horizontality simpliciter" approach and personality rights: Outlining an integrated and constitutional reading strategy to the law of personality *De Jure* (2022) 126.
[31] Ibid.

Given the multiple sources of law that govern the law of personality, an integrated single system reading strategy which is subject to constitutional control premised on the doctrine of the adjudicative subsidiarity together with the horizontality simpliciter approach shall be used to give effect to the POPI Act in relation to determining the requirements that constitute informed consent when personal information is collected by means of a click of a button via cookies.

It is important to note that the doctrine of adjudicative subsidiarity embraces the horizontal application of the Bill of Rights[32] pursuant to s 8(1), 8(2), 8(3) and 39(2) of the Constitution. [33]

Section 8(1) of the Constitution applies to all law and all those who apply it.[34] Whereas, s 8(2) provides that all persons are bound by the provisions of the Bill of Rights if and to the extent that they are applicable, taking into consideration the nature of the right and any duty imposed by those rights.[35] Further, s 8(3) of the Constitution empowers courts when applying the Bill of Rights to, give effect to a right, develop the common law to the extent that legislation does not give effect to that right and may develop common law rules to limit the right in terms of the Constitution. In addition, s 39(2) of the Constitution provides that when interpreting the Bill of Rights, our courts must promote constitutional values, must consider international law and may consider foreign law.[36]

The effect of the latter provisions was uplifted by Chaskalson J in the case *Pharmaceutical Manufacturers Association of South Africa and Another: In re Ex Parte President of the Republic of South Africa and Others*,[37] in which he commented that '[t]here is only one system of law. It is shaped by the Constitution, which is supreme law, and all law, including the common law, derives its force from the Constitution and is subject to constitutional control'. To this effect, when evaluating the fundamental rights at issue and the constitutional values, Bhana notes that sections 8 and 39 of the Constitution form what she terms a "constitutional backdrop".[38] She outlines that s

[32] E Zitzke op cit note at 268.
[33] T Bonongwe *Revenge Pornography, Privacy and Dignity: A Constitutional Analysis of South African Privacy Laws* (unpublished LLM Research Report, Witwatersrand University, 2021) 5-6.
[34] Ibid.
[35] Ibid.
[36] Ibid.
[37] 2000 (2) SA 674 para 44.
[38] D Bhana 'The horizontal application of the Bill of Rights: A reconciliation of sections 8 and 39 of the Constitution' (2013) *South African Journal on Human Rights* 364.

39(2) embodies a broader application of the common law in the constitutional era, by interpreting its rules against constitutional values found in the Constitution.[39] Her thesis entails that when evaluating the horizontal application of fundamental rights in private relationships, constitutional values need to be taken into account..[40] Therefore, it is submitted that the constitutional backdrop to assessing consent as outlined in the POPI Act refers to the constitutional value of human dignity and the fundamental right to privacy.

Visser re-affirms Bhana's position by noting it as horizontality simplicity approach in that the Constitution's horizontality provisions are read together with proposed measures to promote constitutional transformation in line with the aims of the Constitution.[41] By adopting this approach, Visser suggests that the common law doctrine 'ought to function as the starting block for transformative constitutional shifts in private relationships'.[42]

Turning over to the practical application of principle of the doctrine of adjudicative subsidiarity. As a starting basis, all disputes will begin by identifying the constitutional right that has been infringed by an alleged wrongdoer.[43] This leads me to the SANDU-principle derived from the case of *South African National Defence Union v Minister of Defence and Others*[44]. In this case, the Constitutional Court held if a constitutional right is alleged to have been infringed, the dispute must be adjudicated in accordance with legislation promulgated to give effect to that right. As a result, legislation cannot be ignored by direct application of the Constitution.[45]

Zitkse points out that legislation may be circumvented in an instance when such legislation is constitutionally invalid in terms of s 172 of the Constitution.[46]

The second principle is encapsulated as the Bato Star principle derived from the case of *Bato Star Fishing (Pty) Ltd v Minister of Environmental Affairs and Tourism and Others*[47] in which the Constitutional Court held that a litigant ought to rely on

[39] Ibid at 371-372.
[40] Ibid at 372.
[41] CJ Visser 'Adjudicative subsidiarity, the "horizontality simpliciter" approach and personality rights: Outlining an integrated and constitutional reading strategy to the law of personality' *De Jure* (2022) 135.
[42] CJ Visser 'Revisiting the Constitutionalisation of the Common Law of Personality: transformative constitutionalism and Le Roux v Dey' *South African Journal on Human Rights* at 250.
[43] E Zitzke op cit note 28 at 286.
[44] 2007 (5) SA 400 (CC).
[45] Ibid at paras 51-52.
[46] E Zitzke op cit note 28 at 287.
[47] 2004 (4) SA 490 (CC).

legislation expressly enacted to establish a cause of action as opposed to relying directly on the Constitution or common law.[48] The Bato Star principle is subject to the proviso that if legislation does not cover the dispute in question, then common law or customary law act as "safety net" to adjudicate the dispute.[49] By implication, Zitzkse states that this goes further than merely developing the common law against the objects of s 39(2) of the Constitution, but it may involve simply applying the common law principles pursuant to the court's discretion set out in s 173 of the Constitution.[50]

In addition to the above principles, Visser comments that though to a limited extent, common law can nevertheless be considered where legislation is applicable. This is particularly true if common law can provide context for and aid in the interpretation and application of legislative provisions.[51]

Taking into consideration the above, in this paper, it is submitted that the adjudication of privacy concerns implicated by collection of personal information by way of cookies will be adjudicated by application of the POPI Act. In the subsequent sections, the author will discuss sources of law to be referenced as constitutional backdrop instruments, based on informational privacy originating from common law and the GDPR, to give effect to the POPI Act.

III DATA PROTECTION IN SOUTH AFRICA

(a) Introduction and overview of the Protection of Personal Information Act

In the prior section, I discussed that whenever a fundamental right in a dispute between private individuals such dispute must adjudicated in terms of 'legislation that has been specifically enacted to protect the right concerned,' according to the guideline introduced by the notion of adjudicative subsidiarity.[52]

The aim of the POPI Act is to give effect to the right to privacy as guaranteed by s 14 of the Constitution by protecting personal information when it is processed by

[48] Ibid para 25.
[49] E Zitzke op cit note 28 at 287.
[50] Ibid.
[51] CJ Visser op cit note 41 at 249. See T Bonongwe op cit note 33 at 8.
[52] T Bonongwe op cit note 33 at 12.

a responsible party.[53] This is subject to the limitation clause in s 36 of the Constitution, particularly in relation to the right to access to information and the free flow of information within South Africa and abroad.[54] In order to achieve its aims, the POPI Act regulates the manner in which personal information is processed by establishing minimum thresholds for lawful processing which are in harmony with "international standards".[55]

The POPI Act draws inspiration from international guidelines and conventions, such as the OECD Guidelines and the Council of Europe's Convention for the Protection of Individuals concerning the Automatic Processing of Personal Data. These sources emphasise fundamental principles encompassing data collection, purpose specification, use limitation, security safeguards, openness, individual participation and accountability.

The preamble of the POPI Act makes it clear that its provisions are concerned with the regulation of informational privacy as opposed to a broader conception of privacy.[56]

This section will analyse the fundamental provisions of the POPI Act concerning its application to cookies and the relationship with consent. Below, I outline some important concepts as defined in the POPI Act.

(b) Definitions and fundamental concepts

The POPI Act defines "Personal Information: as:

> 'information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including…
>
> (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person'.[57] (own emphasis)

[53] Section 2 of the POPI Act
[54] Ibid.
[55] Ibid.
[56] The preamble of the POPI Act recognises that right to privacy includes a right to protection against unlawful collection, retention, dissemination and use of personal information.
[57] Section 1 of the POPI Act.

The POPI Act further defines “Online Identifier” (unique identifier) as”

> ‘any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party for the purposes of the operations of that responsible part and that uniquely identifies that data subject in relation to that responsible party’.[58]

Further, the POPI Act defines “Processing” as:

> ‘any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including-
> (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
> (b) dissemination by means of transmission, distribution or making available in any other form; or
> (c) merging, linking as well as restriction, degradation, erasure or destruction of information’.[59] (own emphasis)

Further, a “Responsible Party” is defined by the POPI Act as:

> ‘a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information’.[60]

The POPI Act’s definition of processing is wide enough to include a number of functions within the capability of third party cookies, as indicated in the introductory section. In this regard, De Stadler et al comment that when responsible parties use third party cookies, they collect personal information from another source other than directly from the data subject.[61]

The author has pointed out that the POPI Act only applies when personal information is processed if: (i) information can identify the data subject, (ii) information can be linked by a reasonable method which can identify the data subject, or (iii)

[58] Section 1 of the POPI Act.
[59] Section 1 of the POPI Act.
[60] Section 1 of the POPI Act.
[61] De Stadler et al *Overthinking the Protection of Personal Information: The last book you will ever need* op cit note 7 at 299.

information can be modified using a reasonable method to identify the data subject.[62] As defined in s 1 of the POPI Act, personal information includes online identifiers. Identifiers are described as including IP addresses, cookie identifiers, radio frequency identification (RFID) tags, tracking pixels, device fingerprints, MAC addresses, advertising IDs and account handles.[63] On this basis, it is clear that cookies fall within the purview of the POPI Act's definition of personal information.

Processing of personal information must meet minimum threshold requirements based on conditions set out in the Act.[64]

Chapter 3 of the POPI Act enlists eight conditions for information to be processed lawfully. The conditions are as follows: (i) accountability,[65] (ii) processing limitation,[66] (iii) purpose specification,[67] (iv) further processing limitation,[68] (v) information quality,[69] (vi) openness,[70] (vii) security safeguards[71] and (viii) data subject specification.[72] The conditions must be viewed collectively to determine whether personal information is processed lawfully.[73] According to Katzav, the eight conditions symbolise the legislature's intention to 'give effect to the right to privacy'.[74]

As will be demonstrated in the discussion hereunder, this paper is concerned with the second condition of processing of personal information, processing limitation, which encompasses the requirement for consent.

In line with informational privacy, consent provides valid legal basis upon which a responsible party may collect, use, or disclose personal information in compliance with the Act.[75] These justifications ensure that the processing of personal information is carried out transparently and respects the rights of the data subjects. It is important to note that consent is not the sole basis for justifying personal data processing under

[62] Ibid at 298. See also s 12 of the POPI Act.
[63] Ibid.
[64] T Bonongwe op cit note 33 at 13.
[65] Ibid. See s 8 of the POPI Act.
[66] Ibid. See s 9 to 12 of the POPI Act.
[67] Ibid. See s 13 to 14 of the POPI Act.
[68] Ibid. See s 15 of the POPI Act.
[69] Ibid. See s 16 of the POPI Act.
[70] Ibid. See s 17 to 18 of the POPI Act.
[71] Ibid. See s 19 to 22 of the POPI Act.
[72] Sections 23 to 25 of the POPI Act.
[73] Gilad Katzav 'Compartmentalised data protection in South Africa: The right to privacy in the Protection of Personal Information Act' (2022) *SALJ* 443.
[74] Ibid.
[75] Section 11 of the POPI Act.

the POPI Act.[76] Website owners may also process personal information in the following instances: (i) if processing is necessary to carry out obligations in terms of a contract to which a data subject is party,[77] (ii) if processing complies with obligations imposed by the law,[78] (iii) if processing protects a legitimate interests of a data subject,[79] (iv) if processing is necessary for the proper performance of a public law duty by a public body,[80] or (v) if processing is necessary for pursuing the legitimate interest of the responsible party or a third party to whom the information is supplied.[81]

(c) The POPI Act and Cookies: An Analysis of Consent

The POPI Act defines consent as:

> 'voluntary, specific and informed expression of will in terms which permission is given for the processing of personal information'.[82]

The definition of consent presupposes the following elements of consent:

- Voluntary;
- Specific;
- Informed; and
- Expression of will.[83]

(i) Elements of Consent

The POPI Act does not explain or define the elements of consent. The provisions are still unclear. This research paper will attempt to use the integrated reading approach to interpret conditions for consent in light of the use of cookies to collect personal information.

---

[76] Yvonne Burns and Ahmore Burger-Smidt op cit note 8 at 93.
[77] Section 11(1)(b) of the POPI Act. See T Bonongwe op cit note 33 at 14.
[78] Section 11(1)(c) of the POPI Act. See T Bonongwe op cit note 33 at 14.
[79] Section 11(1)(d) of the POPI Act. See T Bonongwe op cit note 33 at 14.
[80] Section 11(1)(e) of the POPI Act. See T Bonongwe op cit note 33 at 14.
[81] Section 11(1)(f) of the POPI Act. See T Bonongwe op cit note 33 at 14.
[82] Section 1 of the POPI Act. A ground of justification in terms of the POPI Act refers to a valid legal basis upon which a responsible party may collect, use, or disclose personal information in compliance with the Act. These justifications ensure that the processing of personal information is carried out transparently and respects the rights of the data subjects.
[83] De Stadler et al *Overthinking the Protection of Personal Information: The last book you will ever need* op cit note 7 at 66-69.

Below, the author discusses provisions related to cookies to understand their implication in attempting to answer the critical questions raised in this paper.

(ii) Special provisions related cookies

Section 57(1) of the POPI Act provides that:

> 'The responsible party must obtain prior authorisation from the Regulator[84]…prior to any processing if that responsible party plans to –
>
> (a) Process any unique identifiers of data subjects –
>
> (i) for a purpose other than the one for which the identifier was specifically intended at collection; and
>
> (ii) with the aim of linking the information together with information processed by other responsible parties'. (own emphasis)

The requirement for prior authorisation was taken from the now repealed EU Data Protection Directive 95/46/EC. This requirement obliged member states to determine which processing operations that were likely to present risks to the rights and freedoms of data subjects.[85]

It is evident from the above that the drafters of the POPI Act took the requirement further by specifying prior authorisation when "identifiers" (which include cookies) are used to collect information, which inclusion can be indicative of the risks associated with their use. Aligned to this is the concern previously raised by the South African Law Reform Commission (SALRC) regarding the potential storage of cookies on an individual's device without obtaining their consent and the subsequent transmission of previously stored information back to the originating website.[86] However, important to note that the POPI Act stipulates that prior authorisation must be obtained by the responsible party just once, not every time personal information is processed.[87]

I argue that the implication of the requirement for prior authorisation does not negate the requirement for consent under the POPI Act, and therefore, the responsible

[84] The Information Regulator is a juristic person established in terms of s 39 of the POPI Act.
[85] Article 20 of the EU Data Protection Directive 95/46/EC.
[86] South African Law Reform Commission Discussion Paper 109 (Project 124) *Privacy and data protection* (2005) para 2.8.
[87] Section 57(4) of the POPI Act.

party is not exempted from proving that it obtained consent prior to processing personal information using unique identifiers.

In summary, while the POPI Act constitutes a momentous advancement in South Africa's landscape of data protection, certain areas such as consent, necessitate further scrutiny and refinement, particularly concerning the regulation of cookies. In the next section, I will discuss the common law conception of common law consent as a way to canvass the elements that could be developed to effect consent in the context of informational privacy.

III Common Law Consent

In this section, I will discuss common law consent and its relationship to informational privacy. I will begin by assessing how case law has developed the concept of common law consent. Additionally, I assess whether there is a connection between common law consent and the Constitution. I will use my analysis to determine what elements of common law consent can be developed to interpret the POPI Act when considering the threshold for consent.

The maxim *volenti non fit iniuria* originates from Roman and Roman-Dutch law.[88] South Africa continues to apply this maxim and its principles.

Innes CJ in the case of *Waring & Gillow Ltd v Sherborne*[89] summed up the nature and characteristics of the defence of *volenti non fit iniuria* as follows:

> 'The *maxim volenti non fit iniuria* embodies a principle which, when confined with right limits, is both just and equitable. A man who consents to suffer an injury can as a general rule have no right to complain. He, who knowing and realising a danger, voluntarily agrees to undergo it, has only himself to thank for the consequences. But like so many other maxims, the one under consideration needs to employed cautiously and with circumspection. The principle is clear; the difficulty lies in the application of it – in deciding, in other words, under the circumstances of each case whether the injured was *volens* to undertake the risk. A consideration of the grounds upon which the doctrine rests, and of the cases in which its scope has been discussed, leads to the

[88] Max Loubser et al *The Law of Delict in South Africa* 3 ed (2017) 204.
[89] 1904 TS 340 at 344.

conclusion that in order to render the maxim applicable it must be clearly shown that the risk was known, that it was realised and that it was voluntarily undertaken. Knowledge, appreciation, consent – these are the essential elements; but knowledge does not invariably imply appreciation, and both together are not necessarily equivalent to consent…'

The following characteristics for valid consent have been extrapolated from case law:

(i) An express indication by the plaintiff that they accept that they would suffer harm or risk of harm. A defendant that not have to show that there is was an agreement with the plaintiff to grant consent.[90] Further, it is not necessary for the defendant to prove willingness of the plaintiff to suffer the harm. Important to note that the plaintiff may invoke the defence of consent at any time prior to the harm being caused.[91]

(ii) The defendant must have been given consent expressly. In other words, there needs to be an external sign of consent.[92]

(iii) Consent can be granted orally either expressly, tacitly or implied. This includes encouragement or invitation to give consent.[93]

(iv) Consent must be obtained before the harm ensued.[94] In this regard, Loubser *et al* note that a defendant may waive their right to claim damages unilaterally or by concluding an agreement with the defendant not to claim if harm is suffered before consent is obtained.[95]

(v) The person who is granting consent must be capable of expressing their will and such consent must relate to the harm.[96] This does not necessarily refer to the extent of capacity or majority status of a defendant.[97] The plaintiff must appreciate the nature and extent of the harm that may ensue.[98] In instances involving a minor who cannot

[90] Max Loubser et al *The Law of Delict in South Africa* op cit note 88 at 205.
[91] Ibid.
[92] Ibid.
[93] Ibid at 206.
[94] Ibid at 206.
[95] Ibid at 206.
[96] Ibid at 206.
[97] Ibid at 206.
[98] JC Van Der Walt and JR Midgley *Principles of Delict* 4 ed (2005) 209.

express their will a parent or guardian's consent shall suffice.[99] When considering whether the plaintiff has mental capacity, the court will assess the nature and value if the interest affected, age, intelligence, knowledge and experience of the person who consented.[100]

(vi) Consent must be granted voluntarily and freely. In this regard, the court will consider each case on its own merits by applying the following factors: moral and economic pressures that affect a plaintiff's choice.[101]

(vii) In order to furnish their consent, the plaintiff must have been appraised with information relating to the nature and extent of ensuing harm or risk.[102] Loubser et al note that a consenting party must have been appraised with all material aspects of the harm or risk of harm.[103] In Castell v De Greef[104] the court added a requirement that consent must be comprehensive, which includes details on the extent of the transaction and its consequences.[105] It stands that informed consent shall not suffice based on knowledge of a risk of harm alone.[106]

(viii) The plaintiff must have been 'willing to suffer harm' by way of intentional conduct and where there is risk of harm ensuing from dangerous activity.[107] In this regard, the court in *Waring & Gillow Ltd v Sherborne*[108] held that: 'knowledge does not invariably imply appreciation, and both together are not necessarily equivalent to consent'.

(ix) Lastly, consent must be lawful, in accordance with the standard of the legal convictions of the community.[109]

Important to note that the court in *Santam Insurance Co Ltd v Vorster*[110] commented that even though there may be practical difficulties in showing proof of the

[99] Max Loubser et al *The Law of Delict in South Africa* op cit note 88 at 206.
[100] Ibid.
[101] Ibid at 207. See also *Imperial Chemical Industries Ltd v Shatwell* [1965] AC 656-658.
[102] JC Van Der Walt and JR Midgley op cit note 98 at 209.
[103] Max Loubser et al *The Law of Delict in South Africa* op cit note 88 at 207.
[104] 1994 (4) SA 408 (C).
[105] Ibid at 425I.
[106] JC Van Der Walt and JR Midgley op cit note 98 at 210.
[107] Max Loubser et al *The Law of Delict in South Africa* op cit note 88 at 207.
[108] Supra note 89 at 344.
[109] 1973 (4) SA 764 (A) at 778.
[110] Ibid at 781.

nature and extent of proof of consent by assumption of risk, an objective test on a balance of probabilities can be applied to resolve this anomaly.

It is evident from the above discussion that the common law rules provide expansive interpretive principles regarding the maxim *volenti non fit iniuria* which can be useful in giving effect to the POPI Act's definition of consent. Courts will have a significant impact in how they use the common law to develop the POPI Act pursuant to their powers granted in terms of the s 8(3) of the Constitution.

Moving over to the discussion on informational privacy, when dealing with the use of cookies, the concept of informational privacy will guide what information an individual discloses to the public and whether the consent which is presupposed by the click of a button, meets the requirements of *volenti non fit iniuria*, as set out from case law. It is plain that consent may be a defence of data controllers and processors against unjustly possessing or processing of private information belonging to others. However, the conception of human dignity, as afforded by the Constitution, preserves informational privacy.[111] The expectation of self-autonomy also drives this.

Below I delineate the concept informational privacy as one of the aspects of "constitutional backdrop" to give effect to the right to privacy as set out in the POPI Act.

Informational privacy refers to the right or ability of individuals to control the collection, use, and dissemination of personal information about themselves.[112] This concept is rooted in the broader right to privacy, protecting individuals from unwarranted intrusion into their personal lives. Informational privacy concerns the handling of data related to an individual's personal life, including but not limited to their health, financial, biometric, and personal communications. It encompasses issues such as data protection, consent to share personal information, data security, and the right to be forgotten.[113]

[111] *National Media Ltd v Jooste* 1996 3 SA 262 (A) para 271; *NM v Smith* 5 SA 250 (CC) paras 262-263.
[112] David Mcquoid-Mason 'Invasion of privacy: Common law v constitutional delict-does it make a difference?' (2000) *Acta Juridica* 227.
[113] Ibid.

Since consent is concerned with the governance of informational privacy, it is important to reflect how privacy is defined under the common law. Privacy as defined by Neethling is understood as:

> 'a condition of human life characterised by seclusion from the public and publicity. This condition embraces all the personal facts which the person concerned has determined to be excluded from the knowledge of outsiders and in respect of which he or she has the will that they will be kept private'.[114]

With regard to the above, I submit that the conception of informational privacy originated in common law, but it was subsequently adopted in the Constitution. Section 14 of the Constitution entails:

> 'Everyone has a right to privacy, which includes the right not to have –
>
> (a) their person or home seized;
> (b) their property searched;
> (c) their possession seized;
> (d) the privacy of their communication infringed'.

Section 14 of the Constitution does not provide an exhaustive list.[115] The protection afforded by s 14 extends the preservation of privacy and one's ability to dictate who has access to their personal information,[116] also referred to as "informational privacy", similar to the position in common law.

The introduction of the constitutional right to privacy as set out in s 14 of the Constitution complements the common law right to privacy. The common law continues to exist in the ecology of South African law despite the principle of subsidiarity.[117] According to Cachalia and Klaaren, the constitutional text provides a 'normative and interpretive resource for Judiciary' to give interpretive framework for the constitutional right to privacy.[118]

---

[114] J Neethling, JM Potgieter and PJ Visser *Neethling's Law of Personality* 2 ed (2005) 371.
[115] D Mcquoid –Mason op cit note 112 at 250.
[116] Ibid at 227.
[117] Cachalia F and Klaaren J Digitalisation, the 'Fourth Industrial Revolution and the Constitutional Law of Privacy in South Africa: Towards a public law perspective on constitutional privacy in the era of digitalisation' (2021) *Digital Pathways at Oxford Paper Series, no. 14* at 16.
[118] Ibid.

The constitutional right to privacy is based on the foundational values of human dignity, equality and freedom.[119] On numerous occasions, our courts have demonstrated that informational privacy is constitutionally connected to human dignity. In the case of *Khumalo and others v Holomisa*[120], O'Regan J noted this close link in which she held that 'the right to privacy, entrenched in section 14 of the Constitution, recognises that human beings have the right to a sphere of intimacy and autonomy that should be protected from invasion'. This link was later accepted and noted by the court in the case of *NM v Smith*[121] as "inter-dependent" and "mutually reinforcing".

Further, in *Barkhuizen v Napier*[122] the court demonstrated the constitutional connection between informational privacy and dignity, as an aspect that forms part of an individual's autonomy. The court noted that part of an individual's freedom and dignity is the ability to regulate one's affairs, even those that may be to their detriment.[123]

Taking into consideration the court's jurisprudence on constitutional connection between privacy and dignity, it is arguable that an unjustified breach of informational privacy will also amount to a violation of human dignity.[124]

Informational privacy can be used as a constitutional backdrop to interpret and discuss the POPI Act in light of s 39(2) of the Constitution which imposes an obligation on courts to develop constitutional values, in particular human dignity.

In the next section, I discuss the European Union's GDPR to evaluate how consent is interpreted to determine whether the POPI Act offers sufficient protection for online users.

IV COOKIES AND THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION ('GDPR')

[119] Section 1 of the Constitution.
[120] 2002 (5) SA 401 (CC) para 27.
[121] 2007 (5) SA 250 (CC) para 131.
[122] 2007 (5) SA 323 (CC).
[123] Ibid para 57.
[124] *Bernstein v Bester* 1996 (2) SA 751 (CC).

(a) General overview of the GDPR

In the introductory section, the author alluded that one of the key instruments relied on by the drafters to the POPI Act was the General Data Protection Directive 95/46/EC, which was repealed by the General Data Protection Regulation 2016/679 (GDPR) when the POPI Act was adopted. While the GDPR may have introduced new provisions that were not contained in the Directive 95/46/EC, most of the GDPR's provisions overlap with those in the Directive 95/46/EC. This is the basis upon which the GDPR is relevant to the discussion hereunder.

Reference will also be made to the Guidelines on Consent under 2016/679 as endorsed by the European Data Protection Board (formerly known as the Article 29 Working Party). The Guidelines provide an analysis to consent provided in the GDPR in order to ensure practical guidance when complying with the GDPR (with reference to the Article 29 Working Party Opinion 15/2011 on the definition of consent).

The goal of the GDPR is to 'harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities'.[125]

Recital 4 of the GDPR sets out the aims of the GDPR, which reads:

> 'The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality'.

Below, author will delineate important concepts as defined in the GDPR as they relate to cookies and consent.

(b) Definitions and fundamental concepts

The GDPR defines Personal Data as:

> 'any information relating to an identified or identifiable natural person ('data subject'); identifiable persons are those who can be directly or indirectly identified using an identifier such as a name, an identification number, location

[125] Recital 3 of the GDPR.

data, an online identifier, or other factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity'.[126] (own emphasis)

The inclusion of "online identifier" under the expanded list of "identifiers" includes cookies.[127]

The GDPR also defines "Processing" as:

> *'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*'.[128]

The definition of "Processing" under the GDPR is defined in terms to encompass many functions that could be done with personal information, such as collection, storage, and alteration amongst others, of personal information.

(c) Analysis of Consent

The GDPR defines "Consent" as:

> '*freely give, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her*'.[129]

Article 7 and Recital 32 of the GDPR set out conditions on how a data controller[130] must act to comply with the requirement of consent.

The conditions as set out Article 7 are read as follows:

---

[126] Article 4(1) of the GDPR.
[127] *Fashion ID GmbH and Co KG v Verbraucherzentrale NRW e.V* (C-40/17) EU:C:2019:629.
[128] Article 4(2) of the GDPR.
[129] Article 4(11) of the GDPR. See also Article 5 of the ePrivacy Directive (not yet promulgated).
[130] A data controller defined as 'natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'. See Article 4(7) of the GDPR.

'(i) Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

(ii) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

(iii) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

(iii) When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.'

Burns and Burger-Smidt comment that the effect of Article 7 provides the data subject with a greater control on how personal data is processed.[131]

Recital 32 of the GDPR provides the following in relation to what consent includes and how it is obtained:

> 'Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity

[131] Yvonne Burns and Ahmore Burger-Smidt op cit note 8 at 95.

should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided'.

According to Article 4(11) of the GDPR, the following requirements for consent need to be met to justify processing of personal data: (i) freely given (voluntary), (ii) specific, (iii) informed and (iv) unambiguous indication of the data subject's wishes by way of clear affirmation (expression of will).

Below I discuss the requirements for consent in the context of using cookies.

(a) Freely given

This element entails that consent must be freely given by the data subject.[132] "Free" implies the data subject's ability to choose and control the use of the personal data.[133]

If the fulfilment of a contractual obligation or the rendering of a service depends on the consent of a data subject then the consent is not deemed "freely given" where it is not necessary for performance of the contract.[134] In the case of *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V*.[135] the court held that "freely given" entails that a data subject must enjoy 'genuine freedom of choice'.[136] The Working Party's Opinion cautions data controllers against bundling the requirements for consent with the provision of a contract or service. This would seem to be reliance on two lawful bases to process personal data, which would constitute bundling.[137] In this instance, to assess whether there is bundling or not, it would be assessed whether the scope of the contract and the data to be processed requires it for performance.[138]

[132] Rosemary Jay Data Protection *Law and Practice* (2020) 5 ed 274.
[133] See Recital 32 of the GDPR.
[134] Article 7(4) of the GDPR.
[135] (ECLI:EU:C:2019:801).
[136] Ibid para 42.
[137] Supra note 21 at 10.
[138] Ibid.

In the context of cookies, commentators note that free choice in the use of cookies shall only suffice if the data subject can accept some or more, decline some or more cookies.[139] Further, consent shall not considered freely given if access to services and functionalities are subject to storing of information or gaining information.[140]

Lastly, free genuine choice to consent includes the ability of the data subject to withdraw consent, without adverse consequences.[141]

(b) Specific

This element entails that consent must relate to a "specific" purpose. The reason for this requirement is to prevent "blanket consent" which covers all purposes.[142] In the context of cookies, this element requires data controllers to provide specificity of the different types of cookies, including the purposes, retention periods of the personal data and third parties who may be involved.[143] Practically, this would require the data controller to obtain consent prior to purpose for which it is requested.[144]

In the case of *Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*[145] the court held that a specific indication of the data subject has to relate to the processing of the data in question and cannot be inferred from an indication of the data subject's wishes for other purposes.[146] The court noted further that in the case of written request for consent, the request must be distinguishable from other matters which concerns other matters.[147] The reason for this is to prevent function creep and promote granularity in consent requests.[148]

(c) Informed

[139] Yvonne Burns and Ahmore Burns-Smidt op cit note 8 at 12.
[140] Supra note 21 at 12.
[141] De Stadler et al *Overthinking the Protection of Personal Information Act: The last book you will ever need* op cite note 7 at 67.
[142] Ibid at 67.
[143] Yvonne Burns and Ahmore Burns-Smidt op cit note 8 at 95.
[144] Ibid.
[145] (ECLI:EU:C:2020:158).
[146] Ibid para 38.
[147] Ibid.
[148] Supra note 21 at 15.

Under this requirement, the data subject must be provided with sufficient details to allow them to make an informed decision, including withdrawal of consent.[149]

The European Data Protection Board (EDPB)[150] sets out the following minimum information for consent to be "informed":

(i) The identity of the data controllers who are involved in processing the personal data;

(ii) The purpose of the processing function for which the consent is sought;

(iii) The type of personal data to be collected;

(iv) An option for the data subject to withdraw consent;

(v) Whether the information to be collected will be used for automated decision making.[151]

The list above is not meant to be exhaustive, depending on the facts surrounding the request for consent, additional information may be required in order to allow the data subject to exercise informed consent.[152]

Data controllers are also required to use plain language when requesting consent. In general terms, this entails language that is understandable by an average person and not only lawyers.[153] This also entails that the information required for consent may not be bundled with other information or hidden in other conditions.[154]

In the *Orange Romania SA*[155] case the court goes further to note that the information provided by the data controller must inform the data subject of the consequences of consent.[156]

Relevant to the element of "Informed", in the context of cookies, the case of *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW e.V.*[157] the court examined

[149] Ibid.
[150] The European Data Protection Board replaces the Article 29 Working Party. The Working Party is an independent advisory body established in terms of Article 29 of the now repealed Directive 95/46/EC. It is appointed to provide the European Commission with guidance on a range of duties, such as developing and implementing privacy policies and providing guidance on privacy matters by adopting working documents, opinions and recommendations.
[151] De Stadler et al *Overthinking the Protection of Personal Information Act: The last book you will ever need* op cit note 7 at 68.
[152] Supra note 21 at 16.
[153] Ibid.
[154] Ibid.
[155] Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (ECLI:EU:C:2020:158).
[156] Ibid para 40.
[157] (ECLI:EU:2019:629).

the issue of identity of data controllers in relation to identifiers. The court found that the definition of data controller as set out Article 2(d) of Directive 95/46/EC (equivalent of Article 4(7) of the GDPR) is wide enough for two or more persons to be controllers when they jointly determine the processing of personal data even though it may be at different stages.[158] The following factors will be taken into consideration when deciding whether person(s) determine purpose and means of processing of personal data: (i) whether the person is involved in the collection, storing and transmission of personal data, (ii) whether the person has benefitted economically by placements of identifiers resulting in free advertising through collection of person data which may processed without consent of the data subject.[159]

(d) Expression of will

In terms of this requirement, consent must be based on an explicit act, which indicates a clear, unambiguous and affirmative expression of will.[160] According to Roos, the data subject must take deliberate action which signifies consent to processing personal data.[161]

Recital 32 of the GDPR provides further guidance in that expression of will may be written or in the form of an oral statement. Recital 32 further states that silence or inactivity shall not qualify as consent.

To fulfill the requirement of expression of will, the act of giving consent must be distinguishable,[162] and while the GDPR does not prescribe the format of the written or oral statement, the Working Party's Opinion notes that the information must be made available before the personal data is processed.[163] However, the use of pre-ticked boxes or opt-in boxes is discouraged as a form of expressing will.[164] Burns and Burger-

[158] Ibid paras 68-70. See *Unabhanginges Landeszentrum fur Schleswig-Holstein GmbH (C-210/16)* (EU:C:2018:388) para 38. See also H Schultz and W Freedman op cit note 25 at 13-14.
[159] Ibid para 71-72, 80.
[160] De Stadler et al *Overthinking the Protection of Personal Information Act: The last book you will ever need* op cite note 7 at 69.
[161] Annaliese Roos The European Union's Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: Evaluation of Selected "Content Principles" (2020) Comparative and International Law Journal of Southern Africa 15.
[162] Supra note 21 at 20.
[163] Ibid at 20.
[164] Ibid at 18. An opt-in process involves the data subject providing consent by means of an affirmative action, either by selection from yes or no options or making a statement. An opt-out process does not require prior consent but the data subject must express their option to remove the consent that is pre-selected. See Yvonne Burns and Ahmore Burns-Smidt op cit note 8 at 96.

Smidt comment that these methods shall only suffice if the data subject was informed and which 'action would signify consent to cookies'.[165] They point out that affirmative action could be inferred from the options presented to the data subject on a consent request form.[166] Important to note that prior consent is required for the opt-in method whereas opt-out does not require prior consent but the data subject must have an option to request removal from future tracking activities.[167]

As the above discussion illustrates, the GDPR provides expansive analysis of the concept of consent as it relates to the use of cookies. Article 7 and Recital 32 of the GDPR are particularly important for this paper as they outline how consent is to be interpreted given the goals set out in the GDPR. The POPI Act does not contain similar provisions. Commentators note that if the approach adopted in the GDPR is followed regarding requirements of consent and were applied correctly and consistently it 'would resolve many of the issues surrounding the issue of valid consent in the POPIA'.[168]

To conclude this section, I submit that the requirements set out under the GDPR will be used as part of the constitutional backdrop envisaged under s 39(2) of the Constitution which encourages our courts to consider foreign law.

V FINDINGS AND RECOMMENDATIONS

This research report aims to determine the threshold of consent when cookies are used to harvest personal information using the Constitution, common law, the POPI Act and the GDPR. In the preceding sections, I argued that when personal information is gathered from another source under the guise of providing consent by clicking a button or from another source, as it is the case with third-party cookies, this poses a threat to privacy.[169] Practically, the report aims to assess the nature of consent required to comply with the POPI Act as informed by privacy laws. In order to attempt

[165] Yvonne Burns and Ahmore Burns-Smidt op cit note 8 at 95.
[166] Ibid at 96.
[167] Ibid.
[168] Ibid at 219.
[169] See Section One.

a response to the aim of the report, I will briefly reflect on the sections discussed in this paper.

In the introductory section, I defined cookies as a method that collects and stores data based on a user's activity on a website. The author also introduced the risks that could be borne from the use of cookies as a method to collect and process personal information and how this relates to the need for valid consent. The author then mentioned the deficiency that arises from the current reading of the definition of consent as contained in the POPI Act. In this discussion, the author found that cookies, in particular third party cookies, raise critical questions relating to privacy concerns and transparency when personal information is collected and stored without consent or knowledge.

In section two, the author discussed how various sources of law, using the integrated reading approach, can be used to address the gaps that are highlighted in the introductory section. By applying Bhana's concept of "constitutional backdrop" to the various sources of law,[170] the author found using the s 8 and 39 of the Constitution, will promote the constitutional transformation through the aims and values of the Constitution in the private law sphere, as suggested by Visser.[171] This method also ensure that the various sources of law are seen to be part of a single-system of law that advances the supremacy of the Constitution.[172]

The significance of the integrated reading approach bridges the relationship between the POPI Act and other sources of law, this is because the relationship between a data subject (internet user) and responsible party is governed by private law principles.

In section three, the author discussed the POPI Act's concept of consent as it relates to cookies. The discussion in this section confirmed that cookies fall within the ambit of the POPI Act. This is evident in the broad definition of "personal information" which includes "online identifiers", which by implication includes "cookies".[173]

[170] See Section Two.
[171] CJ Visser op cit note 38 at 244.
[172] Supra note 37 para 44. See Emile Zitzke op cit note 28 at 270.
[173] Section 1 of the POPI Act.

Following from this, I found that the POPI Act provides for a definition of consent but it does not provide any provisions which explain the components of consent.

In section four, I discussed the maxim of *volenti non fit iniuria* as a ground of justification against invasion to privacy, as a basis of analysing the relationship between common law consent and informational privacy. From the discussion in this section, and as supported by the theoretical framework outlined in section two, I found that common law principles continue to find application in South African law. Our Constitution places a duty on our courts to develop common law principles by promoting the spirit, purport and objects of the Constitution.[174]

The Constitution Court has confirmed that the common law rules are now subsumed into the Constitution.[175]

Against this analysis, I found that common law rules can give effect to consent as set out in the POPI Act. Important to point out even though the rules were predominantly developed in the context of medical treatment,[176] they would still find application in the question to cookies raised in this paper. The leading case of *Santam Insurance Co Ltd v Vorster*[177] provides the elements of *volenti non fit iniuria* as knowledge, appreciation and consent. The case of *Castell v De Greef*[178] further developed these elements and introduced that consent must be comprehensive taking into consideration the entire transaction, including its consequences.[179] Following from this, on very broad terms, I discussed that informational privacy provides individuals with autonomy and its invasion implicates the value of human dignity. To this end, I argue that the findings on common law supplement my argument for use of common law as a constitutional backdrop when interpreting the POPI Act.

In section five, I discussed the provisions of the GDPR on consent in relation to cookies. As stated in this section reference to the GDPR is necessary given the aims of the POPI Act - to regulate processing of personal information in harmony with international standards.

---

[174] Section 39(2) of the Constitution.
[175] Supra note 37 paras 33-34.
[176] Max Loubser et al *The Law of Delict in South Africa* op cit note 88 at 207.
[177] Supra note 103.
[178] Supra note 98.
[179] Ibid at 425I.

To start off, I found that cookies fall within the ambit of the GDPR's definition of personal data, and the broader definition of "identifiers" which is similar to the provisions in the POPI Act. Moving to consent, the GDPR outlines elements of consent as freely given, specific, informed and unambiguous act.[180] These elements are similar to the elements in the POPI Act. The GDPR contains interpretive provisions which further explain the components which make up valid consent when cookies are used to collect personal information, whereas the POPI Act does not contain comparative provisions of this nature.[181]

The value in reference to the GDPR's provisions is in the developed jurisprudence from the foreign courts following testing of privacy-related legislation as they relate to consent when cookies are used. In this regard, South Africa has not had an opportunity to test the POPI Act.

Against the findings outlined above, below I apply the integrated reading approach as contemplated in this paper against the sources of law, i.e. the common law and GDPR, to give effect to the POPI Act when consent is obtained by a mere click of a button by way of cookies.

To start off, the POPI Act applies to cookies and the examination of consent applies to this Act. Cookies also fits within the Act, as the subject matter of processing. The use of cookies involves collection and processing of personal information. Third party cookies collect and process personal information which can be identified or identifiable.[182] The personal information that could be implicated from the use of cookies (these are outlined in the introductory section) is stored on servers which data controllers (website owners) can determine what happens to the information that is collected, and may be publish this information to third parties.[183]

Central to the principle of "processing limitation" is the requirement for consent. Consent acts as a critical mechanism through which users (data subjects) exercise control over their personal information, granting or withholding permission for its processing based on informed decisions. This framework posits that any processing

[180] Article 4(11) of the GDPR.
[181] Article 7 and Recital 32 of the GDPR.
[182] See Section One.
[183] Supra note 118 para 67; *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 2 SA 451 (A); *NM v Smith* 2007 5 SA 250 (CC) paras 39-41, 43.

of personal data without the explicit consent of the data subject is inherently at odds with the principle of processing limitation. Further, the onus of proof lies squarely with the responsible party, the entity that determines the purpose and means of processing personal information. This responsibility entails demonstrating a legitimate basis for any processing activity undertaken, especially in instances where consent is not obtained. The burden of proof is a critical element that ensures accountability and transparency in the processing of personal data. It compels responsible parties to meticulously assess and justify their processing activities, ensuring that they can provide concrete evidence of their adherence to legal and ethical standards should their actions come into question.

The absence of guiding provisions in the POPI Act leads me to the practical application of the doctrine of adjudicative subsidiarity. I have demonstrated that the POPI Act finds application in this paper, however, it has its shortcomings in adjudicating the question of the manner in which consent is collected by way of cookies. In line with transformative constitutionalism, I argue that the principles in common law be used to give effect to the requirement of consent.

As alluded in this paper, informational privacy is linked to human dignity. The non-consensual collection and processing of personal information will invariably invade human dignity. This is because of the practical application of third party cookies which involves the make-up and disclosure of private facts about a person.[184]

Further, I argue that constitutional backdrop in the form of foreign law will be useful in giving effect to the POPI Act. The rules in the GDPR detail how consent is to be interpreted. These rules have been tested by foreign courts. Even though foreign law is not binding in South Africa, it is certainly persuasive.

Against the above discussion, I recommend the following:

(i) Introduction of regulations for website owners (responsible parties) to disclose their identities, including the identities of any third parties that may be hosted on their website for purposes of collecting personal information. This will ensure that internet users are taken into their confidence when interacting with websites. This will further promote transparency amongst

[184] See Section One.

the website owner and internet users. This requirement can act as a foundational step towards establishing a more trustful relationship between internet users and website operators. By mandating the disclosure of not only the identities of website owners (or responsible parties) but also of any third parties with whom they share or from whom they collect personal information, a layer of accountability is added. This approach aligns with global trends towards greater data protection and offers users the ability to make informed decisions about their interactions online. Additionally, such regulations could include stipulations on how and where this information should be presented (e.g., through easily accessible privacy policies or dedicated sections within websites) to ensure that disclosures are user-friendly and not buried in legal jargon.

(ii) Introduction of regulations to guide website owners on obligations to provide internet users with clear and concise information about the types of cookies used on their websites and the purposes for which they are used. Cookies, being pivotal for personalized user experiences, can also raise concerns over privacy and the extent of data collection. Regulations could mandate that website owners not only disclose the types of cookies used but also explain their purpose in plain language. This would enable users to make informed choices about their privacy preferences. For example, distinctions between strictly necessary cookies, functionality cookies, and targeting or advertising cookies should be made clear, alongside options for consent management. This approach promotes a balance between personalized user experiences and individual privacy rights.

(iii) Introduction of the following similar provisions within the body of the Act:

a. Conditions for consent. The GDPR's Article 7 serves as a good example. These conditions spell out how consent is obtained. This includes requirements for making requests for consent in a manner that is clearly distinguishable from other matters, using clear and plain language, and ensuring that the data subject can withdraw consent easily.

b. Supporting conditions for consent. The GDPR's Recital 32, 42 and 43 are good examples. These provisions set out particular instances relating to consent, for instance consent when personal information is processed by automated means, how burden of proof of consent from

data controllers is determined and how “freely given consent” is interpreted.

(iv) Our courts should apply the integrated reading approach by using adjudicative subsidiarity as envisaged by s 8 and 39 of the Constitution to adopt a consent checklist inspired by the common law rules and GDPR’s standards. This checklist would ensure businesses provide clear disclosure and opt-in choices to data subjects, upholding both privacy and human dignity. This checklist would serve as a practical tool for businesses to ensure their compliance with the nuanced requirements of valid consent under both South African common law and GDPR standards. The ultimate aim of introducing such a checklist is to uphold the principles of privacy and human dignity, core values enshrined in the South African Constitution. By requiring businesses to provide clear disclosure and opt-in choices, the legal framework would empower individuals with greater control over their personal information, reinforcing their autonomy and dignity in the digital space.

VI CONCLUSION

The expansion of information technology to enable instantaneous ability of users to interact with social media and the internet challenges the norms of privacy, opens users to abuse and establishes new legal issues calling for a need to maintain transparency.[185]

The research focuses on consent when third party cookies are used to collect personal information. Consent occupies a pivotal role in the legitimate processing of personal information. I highlighted that the POPI Act as the main operative enacted legislation had to be consulted to assess consent. In turn, I found that the POPI Act’s provisions lacked interpretive tools to give effect to consent, as defined, in relation to collection of personal information by way of cookies.

I discussed how the various sources of law, being the common law and the GDPR can be integrated as constitutional backdrops to give effect of the POPI Act.

[185] Richardson M *Advanced Introduction to Privacy Law* 1st ed (2020) 1.

In my analysis, I found a conspicuous disparity emerges between the consent prerequisites elucidated in the GDPR and those delineated in the POPI Act, as seen in the prior discussions. The GDPR sets a threshold for valid consent, accentuating the necessity for detailed conditions for consent, whereas the POPI Act does not impose such exacting specificity. This incongruity underscores the imperative to harmonise South Africa's legislation with international benchmarks and contemplate revising the POPI Act to furnish more explicit provisions governing consent and explicit consent in the processing of special personal information.

It is evident that, for the POPI Act to effectively achieve its objectives of safeguarding the informational privacy of data subjects in the context of cookie usage by data controllers, amendments must be made to align it with international standards such as the GDPR. Harmonising the Act with these standards is crucial to ensure consistency and compatibility with global best practices in data protection.[186]

Lastly, I submit that a need for the threshold for consent when personal information is collected and processed through cookies can assist the development of the law of personality and cyber law.

[186] Mncube N, Ncube T & Ncube B 'Evaluating the POPI Act against international data protection principles: A critical perspective' (2017) 19(1) *South African Journal of Information Management* 4.

BIBLIOGRAPHY

BOOKS:

Boberg, PQR *The Law of Delict* (Juta, Cape Town; 1984).

Burns Y and Burger-Smidt, A *Protection of Personal Information Law and Practice* 2 ed (LexisNexis, Johannesburg; 2023).

De Stadler, E et al *Over-thinking the Protection of Personal Information Act: The last book you will ever need* (Juta, Cape Town; 2021).

Jay, R *Data Protection Law and Practice* 5 ed (Sweet & Maxwell, London; 2020).

Loubser, M et al *The Law of Delict in South Africa* 3 ed (Oxford University Press, Cape Town; 2017).

Neethling, J; Potgieter, JM and Visser, PJ *Neethling's Law of Personality* 2 ed (Butterworths, Durban; 2005).

Neethling, J; Potgieter, JM and Visser, PJ *Law of Delict* 8 ed (LexisNexis, Johannesburg; 2020).

Van Der Merwe, D et al *Information and Communication Technology Law* 2 ed (LexisNexis, Johannesburg; 2016).

Van Der Walt, JC and Midgley, JC *Principles of Delict* 4 ed (LexisNexis, Durban; 2016).

JOURNAL ARTICLES:

Bhana, D 'The horizontal application of the Bill of Rights: A reconciliation of sections 8 and 39 of the Constitution' (2013) 129 *South African Journal on Human Rights* 351.

Cachalia, F and Klaaren, J 'Digitalisation, the Fourth Industrialisation Revolution and the Constitutional Law of Privacy in South Africa: Towards a public law perspective on constitutional privacy in era of digitalisation' (2021) 14 *Digital Pathways of Oxford Paper Series* 1.

Cachalia, F and Klaaren, J 'Towards a Public Law Perspective on the Constitutional Law of Privacy in South Africa in the Age of Digitalisation' (2023) *Journal of African Law* 1.

Ebersohn, G 'Internet law: cookies, traffic data and direct marketing practices' (2004) 16(4) *SA Mercantile Law Journal* 741.

Freedman, W and Schultz, H 'Plugins and POPI: A Critical Discussion into the Legal Implications of Social Plugins and the Protection of Personal Information' (2023) 26 *PER/PELJ* 1.

Harthorne, L 'Legal tradition and the transformation of orthodox contract theory: The movement from formalism to realism' (2006) 12(2) *Fundamina* 83.

Hermann, B and Papadopoulos, S 'Direct Marketing and Spam Via Electronic Communications: An Analysis of the Regulatory Framework in South Africa' (2014) 47(2) *De Jure* 42.

Katzav, G 'Compartmentalised data protection in South Africa: The right to privacy in the Protection of Personal Information Act' (2022) 139(2) *South African Law Journal* 432.

Mcquuoid-Mason, D 'Invasion of Privacy: Common Law v Constitutional delict – does it make a difference?' (2000) *Acta Juridica* 227.

Mncube, N; Ncube, T and Ncube, B 'Evaluating the POPI Act against international data protection principles: A critical perspective' (2017) 19(1) *South African Journal of Information Management* 1.

Roos, A 'The European Union's Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: Evaluation of Selected

"Content Principles"' (2020) 53(3) *Comparative and International Law Journal of Southern Africa* 1.

Visser, CJ 'Revisiting the Constitutionalisation of the Common Law of Personality: transformative constitutionalism and Le Roux v Dey' (2020) 36(2) *South African Journal on Human Rights* 242.

Visser, CJ 'Adjudicative subsidiarity, the "horizontality simpliciter" approach and personality rights: Outlining an integrated and constitutional reading strategy to the law of personality' (2022) 55(1) *De Jure* 1.

Zitske, E 'Constitutional heedlessness and ever-excitement in the common law of delict's development' (2015) 7 *Constitutional Court Review* 259.

TABLE OF CASES:

Barkhuizen v Bester 1996 (2) SA 751.

Bato Star Fishing (Pty) Ltd v Minsiter of Environmental Affairs and Tourism and Others 2004 (4) SA 490 (CC).

Bernstein v Bester 1996 (2) SA 751.

Castell v De Greef 1994 (4) SA 408 (C).

Financial Mail (Pty) Ltd v Sage Holdings Ltd 1993 2 SA 451 (A).

Khumalo and Others v Holomisa 2002 (5) SA 401 (CC).

National Media Ltd v Jooste 1996 (4) SA 408

NM v Smith 5 SA 250 (CC)

Santam Insurance Co Ltd v Vorster 1973 (4) SA 764 (A).

South African National Defence Union v Minister of Defence and Others 2007 (5) SA 400 (CC).

Waring & Gillow Ltd v Sherborne 1904 TS 340.

TABLE OF FOREIGN CASES:

Fashion ID GmbH and Co KG v Verbraucherzentrale NRW e.V (C-40/17) EU:C:2019:629.

Imperial Chemical Industries Ltd v Shartwell [1965] AC 656.

Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. (ECLI:EU:C:2019:801).

Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (ECLI:EU:C:2020:158).

THESES AND RESEARCH REPORTS:

Bonongwe T '*Revenge Pornography, Privacy and Dignity: A Constitutional Analysis of South African Privacy Laws* (unpublished LLM Research Report, Witwatersrand University, 2021).

Silva, CC '*Consumer evaluation of cookies for marketing purposes: Case Study for Portuguese Consumers*' (unpublished Information Management thesis, Nova University Lisbon, 2021).

Visser, CJ '*Human Dignity and Actio Iniuriarum: A Constitutionalised Approach to Personality Infringement*' (unpublished LLD thesis, University of Witwatersrand, 2020).

TABLE OF STATUTES AND PARLIAMENTARY DOCUMENTS:

Constitution of the Republic of South Africa, 1996.

Protection of Personal Information Act 4 of 2013.

South African Law Reform Commission Discussion Paper 109 Privacy Data Protection (October 2005).

FOREIGN TABLE OF STATUTES AND PAPERS:

Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679 WP259 rev.1.1 (4 May 2020).

General Data Protection Directive 95/46/EC.

General Data Protection Regulation 2016/679.

Weeransinghe, SDRM 'Paper on Cookies, Privacy and Cyber Security' (2019) University of Moratuwa Sri Lanka.

INTERNET SOURCES

CookiePro Knowledgebase 'What is a cookie?', available at *https://www.cookiepro.com/knowledge/cookie-wall/#:~:text=Essentially%2C%20a%20cookie%20wall%20is%20a%20variation%20of,a%20cookie%20wall%20is%20a%20notice-only%20banner%20below*, accessed on 24 February 2021.

Herman P 'The Cookiepocalypse: Why first-party data is going to matter to your newsroom' available at *https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2022-09/RISJ%20Paper_Paul%20H_TT22_Final_1.pdf*, accessed on 13 February 2024.

Komnenic M 'First-Party vs. Third-Party Cookies: The Differences Explained' available at *https://termly.io/resources/articles/first-party-cookies-vs-third-party-cookies/*, accessed on 13 February 2024.

Michalsons 'Cookie law in South Africa', available at *https://www.michalsons.com/blog/cookie-law-south-africa/15264*, accessed on 8 October 2023.

Microsoft 'Everything you need to know about Internet cookies', available at *https://www.microsoft.com/en-us/edge/learning-center/what-are-cookies?form=MA13I2*, accessed on 17 March 2024.

The ICO 'Guidance on the Use of Cookies and Similar Technologies' available at *https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-cookies-and-similar-technologies/#cookies1*, accessed on 25 February 2024.