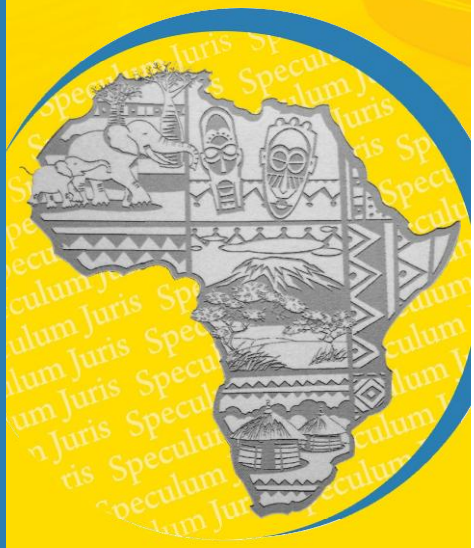
Speculum Juris

Vol 40 No 1 (2026)
Published 31 August 2026

ISSN 2523-2177



Cite as: Rammila *et al.* "Cookies, Legitimate Interests, and Consent: Exploring the Protection of Personal Information in South Africa and the European Union" 2026 (40) Spec Juris 1–16

University of Fort Hare
Together in Excellence

Cookies, Legitimate Interests, and Consent: Exploring the Protection of Personal Information in South Africa and the European Union

D Rammila[*]
Senior Lecturer, Department of Mercantile Law, University of South Africa

N Ntsaluba[**]
Lecturer, Department of Mercantile Law, University of South Africa

Abstract

In today's world, personal information is an extremely important economic resource. With internet access now almost a universal reality, the market for personal data around the world is lucrative. Nearly every company with a digital internet presence collects and processes personal information. The most common method of such collection is through the use of internet website cookies. Cookies are small data files stored on an internet user's web browser (or device) when they visit a website and are used for a wide array of functions inter alia including tracking and recalling of user interactions, tracking of browsing habits and service personalisation. Cookies, as such, can harvest large amounts of data, including personal information, from web users. The law regulating the collection, storage and processing of personal information in South Africa is the Protection of Personal Information Act 4 of 2013 (POPIA). Although the POPIA

[*] LLB, LLM *cum laude,* LLD (University of Johannesburg).

[**] LLB, PBL, MBL (Unisa); LLM–IP & Cyber Law, LLM–Extractive Industries Law (University of Pretoria); BSc, BEd, PGDEd (UNITRA); MEd (UFS).

does not make specific reference thereto, cookies still fall within its scope as it regulates all matters relating to the handling of personal information. This contribution investigates the regulation of cookies under the POPIA and the European Union's (EU) data protection laws, focusing on their role as a primary tool for the collection of personal information. It examines cookie consent request presentations and their compliance with the requirements for lawful processing of personal information, particularly as they relate to questions of consent and legitimate interests under these frameworks. The article concludes that in comparison to the EU's regulatory framework, the POPIA's regulation of cookies is largely deficient.

Keywords: consent; cookies; GDPR; legitimate interests; personal information; POPIA

1 INTRODUCTION

South Africans have a constitutionally protected right to privacy.[1] Section 14 in the Bill of Rights describes the right as including, among others, the right not to have their property seized and, importantly, not to have their communications infringed.[2] Of relevance to the current contribution is what has been described as that "aspect of the general right to privacy that has come to be of considerable practical importance," namely, informational privacy.[3] Informational privacy specifically *inter alia* covers aspects of the collection, utilisation and disclosure of private information, including personal information. In furtherance of the right to privacy, in particular personal informational privacy, the POPIA provides that the right also includes the right to not have one's personal information unlawfully collected, retained, disseminated and used.[4] Neethling and Potgieter conceptually define privacy as an "individual condition of life that is characterised by seclusion from the public and publicity."[5] It is said to "embrace all those personal facts which a person chooses to exclude from the knowledge of others and in respect of which that person is entitled and so wishes to be kept private."[6] Privacy as a legal condition "embraces … those personal facts [of] which … [a] person … has determined must be excluded from the knowledge of outsiders, and [of] which [they wish] … to be kept private."[7]

What the right entails is an entitlement to be left alone[8] — to be able to live one's life with a level and degree of freedom and personal security beyond the interference or unsolicited influence of outside persons.[9] Like many other rights in the Bill of Rights, however, it is not without its limits.[10] Where the person decides to waive that aura of discreetness and inviolability through interactions with others, that condition, being the entitlement to privacy of that person, becomes subject to limitations.[11] This fact, however, does not mean that the person concerned forfeits the protection of his right to privacy.

1 Constitution of the Republic of South Africa, 1996, s 14.

2 *Ibid*.

3 Nxokweni "Protection of Informational Privacy in the Workplace Given the Advancement in Technology" 2024 *Obiter* 199 202.

4 Preamble of Act 4 of 2013.

5 Neethling, Potgieter and Visser *Law of Personality* (2005) 32.

6 *Ibid*.

7 Nxokweni *Legal Principles Regulating the Processing of Personal Information in the Workplace* (LLM-Dissertation, Unisa, 2018) para 8.

8 *NM and v Smith* 2007 5 SA 250 (CC) para 32.

9 *Ibid* para 33; see also *Bernstein v Bester* 1996 2 SA 751 (CC) para 77.

10 Section 36 of the Constitution provides that the rights in the Bill may be limited by a law of general application taking into account various relevant factors; see also Mthembu "Marriage of Convenience: Bank-Customer Relationship in the Age of the Internet: A South African Perspective" 2014 *Journal of International Commercial Law and Technology* 14 22.

11 *Bernstein v Bester* para 77.

What this entails is that the person's claim for protection of this right will now have to be construed through a different lens than would have been the case had they not allowed outsiders to interact therewith.[12] Does this then mean that when a person browses a website, they willingly and unreservedly consent to the collection of personal information in violation of their privacy? In particular, does it mean that the party responsible for the collection of information on such a website and has access to their personal information, or another party related thereto with similar access, can conduct such collection and processing in whichever manner that it pleases?

This contribution investigates the regulation of cookies under the POPIA and European Union (EU) data protection law, focusing on their role as a primary tool for the collection of personal information. EU data protection law obliges data controllers to ensure that cookies are presented in a manner that is accommodative of users' interests. It examines requirements for the lawful processing of personal information, including questions of consent and legitimate interests and considers whether cookies as tools that collect personal information are properly regulated.

2 UNDERSTANDING COOKIES

Data privacy has evolved in several stages and has manifested in various strategies to both collect and protect personal information. One of the most common means by which personal information is collected is by means of cookies.[13] Cookies are small text files that are installed and stored on a user's hard drive by web servers.[14] They are used to store stateful information which web servers can access on the user's device to "remember" the user's browsing activities.[15] As noted above, cookies are text files and can only be used by web browsers. They are not computer executables that can independently run on a user's computer or even access information stored on a hard drive.[16] Cookies are capable of recording such important information as the user has previously entered, including credit card numbers or their address(es).[17] Cookies can also be synchronised with each other and with other application programming interfaces (APIs) to record and infer computer location coordinates, network information and to store unique identifiers of files stored on web servers.[18]

Initially, cookies were used for state management purposes to enhance user experience when browsing by storing session identifiers which allowed users to return to a website and ensure continuity of web sessions.[19] However, their functionalities have expanded to encompass a wide variety of uses including personalisation, analytics, advertising, and tracking.

12 *Ibid*.

13 Tladi *The Regulation of Unsolicited Electronic Communications (SPAM) in South Africa: A Comparative Study* (LLD-Thesis, Unisa, 2017) 40.

14 *Ibid.* See also Axinte *et al.* "Browsers Cookies – An (In)Security Analysis" 2017 *International Journal of Information Security and Cybercrime* 23 25, Oppenheimer "Internet Cookies: When Is Permission Consent" 2006 *Nebraska LR* 383 385.

15 Axinte *et al.* 2017 *International Journal of Information Security and Cybeercrime* 25; see also Hormozi "Cookies and Privacy" 2006 *Information Systems Security* 51; Sipior, Burke and Mendoza "Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons" 2011 *Journal of Internet Commerce* 1 3.

16 Harding, Reed and Gray "Cookies and Web Bugs: What They are and How They Work Together" 2006 *Information Systems Management* 17 18.

17 Oppenheimer 2006 *Nebraska LR* 387; see also Harding, Reed and Gray 2006 *Information Systems Management* 18.

18 Papadopoulos, Kourtellis and Markatos "Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask" in *The World Wide Web Conference (WWW '19), New York, NY, USA* (2019) 1432–1442.

19 Sipior, Burke and Mendoza 2011 *Journal of Internet Commerce* 2.

Cookies today perform various functions including ensuring the efficient operation of websites and provision of services, for tracking and recording user behaviour and preferences during online sessions and for tracking users on other websites, usually by third parties.[20] The tracking functions are especially relied upon by marketers and advertisers to infer user interests in order to provide targeted or highly specific advertisements.[21] Cookies are capable of storing vast amounts of information about a user that may be used to profile and identify them, especially when used in combination with other cookies and web APIs.[22] Cookies may be broadly categorised into two types, namely, session and persistent cookies. Session cookies have a temporary character and are generally used to maintain user session states or remember choices made during web browsing.[23] Once the user closes their browser, session cookies are then deleted from their hard drive. Persistent cookies on the other hand are coded to remain on the user's hard drive long after they have ceased surfing the relevant website.[24] Each persistent cookie has its own expiration date and will be deleted upon such date.[25] Persistent cookies are generally used to store and recall information about user credentials to enable them to automatically log in on sites they previously used, as well as their preferences. However, some persistent cookies can pose serious privacy risks as they are capable of tracking user behaviour across multiple, separate web sessions or entirely different websites.[26]

Cookies may further be subdivided in terms of the purpose each of them serves. The most common type of cookie is known as a strictly necessary cookie. As the name suggests, strictly necessary cookies are essential for the core functionality of websites and their presence is necessary to allow users to access secure features thereof.[27] The second, performance or statistics cookies, are not strictly necessary, but are useful in that they allow websites to collect information about how users interact with websites and their pages.[28] This information is usually unidentified and is used by websites to improve the user experience based on user behaviour. Functionality cookies are used by websites to recall a user's preferences and choices such as their preferred language, region or login information.[29] While not inherently capable of storing identifiable information, functionality cookies can still be used in combination with other cookies storing personally identifiable information and APIs to psychometrically map users and their preferences. Marketing cookies are those cookies which are used to collect vast amount of data including browsing history, preferences and activities across multiple websites.[30] The harvested data can be, and is almost always, shared with third parties and is usually used to deliver targeted advertisements and content based on inferred preferences and behaviour from the information collected.[31]

20 *Ibid* 3.

21 *Ibid* 14; see also Tladi *The Regulation of Unsolicited Electronic Communications* 40.

22 Papadopoulos, Kourtellis and Markatos "Cookie Synchronization" 1433.

23 Oppenheimer 2006 *Nebraska LR* 388; see also Dabrowski *et al* "Measuring Cookies and Web Privacy in a Post-GDPR World" in Choffnes and Barcellos (eds) *Passive and Active Measurement: Lecture Notes in Computer Science* (2019) 258 260.

24 *Ibid*.

25 Dabrowski *et al.* "Measuring Cookies" 260.

26 *Ibid*.

27 *Ibid;* see also Lin *et al.* "Browsing Without Third-Party Cookies: What Do You See?" in *Proceedings of the 2024 ACM on Internet Measurement Conference (IMC '24)* (2024) 130 131.

28 Lin *et al.* "Browsing without Third-Party Cookies" 131.

29 *Ibid*.

30 *Ibid*.

31 *Ibid* 135.

3 COOKIE REGULATION UNDER THE POPIA

Activities relating to the collection, retention and processing of personal information in South Africa are governed by the POPIA. Adopted in 2013, the Act provides the framework for the protection of personal information in the Republic and creates and imposes certain duties on users of personal information.[32] Personal information is broadly defined in the Act to consist of information that relates to living human beings who can be identified therefrom or to "an identifiable, existing juristic person," which information relates, but is not limited, to demographic information *inter alia* including a person's race, gender, colour, age, conscience, belief, language of birth and sexual orientation.[33] Information relating to certain types of sensitive information is also included under the definition of "personal information" and includes a person's educational, medical, financial or criminal history.[34]

The Act further protects information that relates to people's personal opinions and the opinions that others may have about them as well as unique identifiers that a person may be assigned (and accordingly identified by) such as, "any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person."[35] Other information qualified as personal information includes biometric data, private or confidential correspondence, and a person's name "if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person."[36]

From the definition of personal information provided in the Act, one may understand personal information as encompassing aspects of a person's personality, to which they are entitled to keep private and would in the ordinary course of events, prefer to keep confidential. Indeed, Burns and Burger-Smidt confirm that information of a personal nature can be said to "relate to that part of a person's life which he or she does not want divulged to third persons."[37] By its very nature, personal information is inextricably linked to a person's entitlement to privacy which is protected under the Constitution.[38]

Given the nature and, at times, sensitivity of the information concerned, the POPIA imposes several rules regarding the processing of personal information. From the outset,[39] the Act entitles data subjects whose personal information is subject to processing, with a right to have such information processed consistent with the conditions set out in the Act. This entitlement extends but is not limited to the right to be notified in the event of personal information being collected or when a data breach has occurred.[40] Data subjects are also empowered to exercise control, where necessary, over the integrity of their personal information, which power is embodied in the right to request that such information either be corrected, destroyed or deleted.[41]

To this end, the Act provides several conditions for the lawful processing of information. These conditions are listed generally in section 4 of the Act and specifically include accountability, a limitation on processing, purpose specification, further processing limitation, information

32 Section 1 of Act 4 of 2013.

33 *Ibid*.

34 *Ibid*.

35 *Ibid*.

36 *Ibid*.

37 Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* (2023) para 2.4.3.

38 *Ibid*.

39 Section 5 of Act 4 of 2013.

40 *Ibid* s 22(1)(b).

41 *Ibid* s 5(c).

quality, openness, security safeguards and data subject participation.[42] The first — accountability — requires of responsible parties to ensure that, "at the time of the determination of the purpose and means of the processing and during the processing itself," the processing of personal information is conducted consistent with the Act's conditions, including all measures giving effect thereto.[43] The requirement, in general, places the burden of responsibility on the responsible party to ensure that processing is done in compliance with the POPIA. Necessarily, the Act also imposes certain limitations on the processing of personal information.

Section 9 requires that personal information be processed in a manner that is both lawful and does not invade a data subject's privacy while section 10 imposes a data minimisation requirement on the processing of personal information, requiring that personal information be processed only if it is "adequate, relevant and not excessive."[44] Data minimisation is described as entailing the obligation of a responsible party to ensure that "enough personal data … [should be processed] … to reach a correct decision, but not more than is necessary."[45]

A further limitation found in section 11 of the POPIA is the requirement that personal information not be collected without the consent of the data subject or, where the data subject is a child, the consent of a competent person.[46] Section 11 further provides instances whereby personal information may be processed. This includes instances whereby processing is required to conclude or execute a contract to which the data subject is party or if such processing is done in compliance with the responsible party's imposed legal obligation or if it is "necessary for the proper performance of a public duty by a public body."[47] Furthermore, personal information can also be processed if doing so "protects the legitimate interests of the data subject" or serves a necessary purpose in pursuit of the responsible party's legitimate interests or that of another party "to whom the information is supplied."[48]

3 1 The Requirement of Consent

The requirement of consent has been described as "arguably one of the most important … requirements for the lawful processing of personal information."[49] Consent in the Act is defined as entailing a "voluntary, specific and informed expression of will" in any form "in terms of which permission is given for the processing of personal information."[50] Conceptually understood, the definition of consent under the POPIA necessarily requires that a data subject be consulted (in whichever format or avenue) prior to the collection of their data.[51] The requirement for voluntariness means essentially that a data subject should be allowed to make the choice whether to permit processing of their personal information free from any coercion or undue influence or pressure from the responsible party (or any other person for that matter). However, the free expression of one's will does not fully satisfy the definition as provided in the Act. It is further required that such an expression be informed.[52] In other words, the data subject must be properly provided with the relevant information to enable them to understand the responsible

42 *Ibid* s 4.

43 *Ibid* s 8.

44 *Ibid* s 10.

45 Roos "Data Protection Principles Under the GDPR and the POPI Act: A Comparison" 2023 *THRHR* 1 13.

46 Section 11(a) of Act 4 of 2013.

47 *Ibid* s 11(e).

48 *Ibid* s 11(f).

49 Burns and Burger-Smidt *Protection of Personal Information* para 3.3.1.

50 Section 1 of Act 4 of 2013.

51 Burns and Burger-Smidt *Protection of Personal Information* para 3.3.1.

52 Section 1 of Act 4 of 2013.

party's designs for their personal information. In this respect, Burns and Burger-Smidt suggest that a data subject will have made an informed expression of will if they were made "fully aware of all the circumstances and the advantages and disadvantages of processing."[53] It is not clear from the definition of consent under the Act what is meant by "specific … expression of will." Unlike the EU's General Data Protection Regulation (GDPR) which expressly couches consent specificity as amounting to separate consent for distinct processing operations,[54] the POPIA is completely silent on this point. It is indeed possible that consent specificity under the POPIA may simply require of the responsible party to ensure that information about the purpose for each processing operation be specifically and clearly indicated in the consent request, and not necessarily that the data subject be given the opportunity to exercise choice individually, as suggested by the posture of subsections 13(1) and (2). For as long as the POPIA remains silent on this and to the extent that no further guidance is given by the courts, whether separate consent is required under the POPIA will remain open to interpretation. However, the definition of consent under the Act, arguably is capable of being interpreted to require separate consent.

Where a data subject has given their consent, section 11(2)(b) of the Act empowers them to withdraw consent for processing at any time, subject to the condition that any prior lawful processing of their personal information will not be affected thereby.[55] This requirement essentially means that a data subject who opts to withdraw their consent to processing, after having previously permitted it, cannot demand that processing conducted prior to the withdrawal be reversed or otherwise destroyed. In addition, a data subject is allowed to object, in the prescribed manner, to the processing of personal information in instances where such processing is justified on a legitimate interest of theirs or that of responsible parties.[56] It is also possible for a data subject to object to processing when the purpose served thereby is to enable a public body to perform a public duty properly or "for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications as referred to in section 69."[57]

Consent is also important in the context of further processing of personal information. Section 12(1) of the POPIA specifically demands that the collection of personal information be done directly from the data subject.[58] In other words, if a responsible party intends to process information, it needs to collect the same from the data subject. However, section 12(2) qualifies the requirement of direct collection under section 12(1), and specifically provides for various circumstances under which indirect collection of personal information may not be necessary.[59] Of relevance is the proviso specifying that direct collection of information is not necessary if obtaining it from another party is necessary *inter alia* for the administration of justice and national security, and if such collection is necessary for the maintenance of the legitimate interests of the responsible party or a third party.[60]

53 Burns and Burger-Smidt *Protection of Personal Information* para 3.3.1.

54 Article 7(2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC GDPR.

55 Section 11(2)(b) of Act 4 of 2013.

56 *Ibid* s 11(3).

57 *Ibid*.

58 Section 12(1) of Act 4 of 2013.

59 *Ibid* s 12(2) of Act 4 of 2013.

60 *Ibid*.

3 2 A "Legitimate" Interest under the POPIA

Closely related to the requirement for consent is the proviso in respect of legitimate interest. As already noted previously, processing of personal information generally requires a data subject's permission. However, a responsible party can also do so if it would not prejudice the protection of the legitimate interests of the data subject or if it is done in pursuit of its own.[61] Nowhere in the POPIA is a definition of legitimate interest provided. Since no judicial decision regarding the meaning of legitimate interest has been made in South Africa, distilling the same requires regard for lessons from both domestic and international sources. Burns and Burger-Smidt observe that legitimate interests within the context of the POPIA may relate to the business and commercial interests of the parties. They observe that the concept of legitimate interest can be said to have attained legitimacy through its acceptance in common law.[62] Focusing on the meaning of "legitimate", the writers note that the word necessarily entails the condition of being lawful or licit.[63] Thus, where the interest pursued by a responsible party is one that violates the law, it cannot be said to be legitimate. Put differently, there can be no legitimate interest when processing of personal information serves the purpose of attaining an unlawful or illicit outcome or if it is done in contravention of any law. What constitutes an "interest" is what the writers describe as "something less than a right" but one which needs to be properly substantiated and recognised in law.[64] A legitimate interest cannot be a bare expression of an interest as such. Burns and Burger observe in this respect that a legitimate interest must be related to a specific outcome and personal information processing cannot infringe on the fundamental rights and freedoms of a data subject's absent statutory authorisation.[65]

3 3 Cookies in the POPIA

The text of the POPIA does not explicitly refer to web cookies. However, neither does the Act make any specific references to a particular method of personal information collection, of which responsible parties may make use. This is not in itself anomalous as legislation, especially that of a general nature, rarely ever delve into the specificities of the regulated subject matter.[66] In other words, there is generally no specific need for the Act to deal explicitly with an aspect of a regulated issue. However, cookies may engage with a subject matter falling within the definition of personal information.[67] As previously noted, cookies play a significant role in the process of data collection on the internet. In fact, in today's internet-based-and-reliant society, cookies are the most commonly used mechanism for obtaining information from internet users, including information about user behaviour (including preferences), device internet protocol addresses and location.[68] Whether it is for purposes of providing a service or for developing a database of a user's online behaviour so as to match them to services they may be interested in, cookies are one of the most important instruments through which the vast majority of user personal information on the internet may be collected.[69]

61 *Ibid* ss 11(d) and (f).

62 Burns and Burger-Smidt *Protection of Personal Information* para 3.5.2.

63 *Ibid*.

64 *Ibid*.

65 *Ibid* para 3.5.2.1.

66 De Stadler, Hattingh and Esselaar *Over-thinking the Protection of Personal Information Act* (2021) 299.

67 Including online identifiers—see s 1 Act 4 of 2013; see also De Stadler, Hattingh and Esselaar *Over-Thinking the POPIA* 299.

68 Tladi *The Regulation of Unsolicited Electronic Communications* 40.

69 *Ibid*.

Although new technologies capable of performing the same or advanced collection functionalities are being developed and indeed implemented,[70] cookies remain indispensable.

That cookies are covered under the POPIA is generally not in question. Even if the POPIA does not make specific reference thereto, cookies are still subject to its application. The POPIA regulates the processing of personal information including the collection thereof. The method of collection generally does not have an impact on the applicability of the POPIA's provisions.[71] Provided that a method engages personal information, then the application of the POPIA is, by consequence, invited.[72] As such, since cookies are generally geared towards obtaining user information, including the online identifiers and IP addresses of internet users, the POPIA generally will apply thereto. But as already mentioned above, given the prevalence of cookies and their extensive reach, it makes sense that guidance on their usage should at the very least be provided, even if this is done indirectly through regulations regarding the issuing of consent or, preferably, the deployment of cookies. However, notwithstanding the already-noted silence of the POPIA, no such regulation exists in South Africa. Although the subject matter that cookies engage with may be protected and by extension cookies themselves indirectly regulated, how responsible parties should go about obtaining consent for, or under what circumstances their legitimate interests may justify the collection of personal information through cookies, is not.

The silence and clear lack of specific regulation of cookies in South Africa is by no means passable. In their wide-ranging 2024 empirical study of South African e-commerce websites, Da Veiga *et al.* note that compliance with the requirement for consent was notably limited.[73] Of the fifty sites investigated, two-fifths provided an option to accept cookies while 46 per cent did not give users the option to either accept or reject cookies.[74] In respect of consent for third party sharing, virtually all websites did not attempt to properly request consent therefor.[75] In fact, just over a quarter of them made consent for sharing information with third parties compulsory while more than half did not even request consent.[76] On top of that, none of the surveyed websites indicated whether they disclosed information to third parties.[77] When it comes to the source from which personal information is collected, it was not clear how 40 per cent of the surveyed sites collected information while 46 per cent indicated that they used a combination of direct and indirect (third party) collection.[78]

In addition, there is a tendency for websites to present users with binary choices between access and lack of access, conditioned upon the acceptance of cookies that are not strictly necessary for provision of the service sought.[79] This can be done through the use of clickwraps that essentially function as paywalls, with consent to personal data collection being the cost of

70 Ha Dao and Kensuke Fukuda "Alternative to Third-Party Cookies: Investigating Persistent PII Leakage-based Web Tracking" in Association for Computing Machinery *Proceedings of the 17th International Conference on Emerging Networking EXperiments and Technologies (CoNEXT '21)* 223 223–229.

71 De Stadler, Hattingh and Esselaar *Over-Thinking the POPIA* 299.

72 Section 3(1)(a) of Act 4 of 2013; see also De Stadler, Hattingh and Esselaar *Over-Thinking the POPIA* 299.

73 Da Veiga *et al.* "Evaluating Data Privacy Compliance of South African E-Commerce Websites Against POPIA" 2025 *Journal of Information Systems and Informatics* 2693 2706–2712.

74 *Ibid* 2706.

75 *Ibid* 2707.

76 *Ibid*.

77 *Ibid*.

78 *Ibid*.

79 Li "The FTC and the CPRA's Regulation of Dark Patterns in Cookie Consent Notices" 2022 *University of Chicago Buss LR* 561 587; see also Utz *et al.* "(Un)informed Consent: Studying GDPR Consent Notices in the Field" in Association for Computing Machinery *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)* 973 975.

access, obfuscating information and therefore barring access to information entirely.[80] Another technique that websites use is information limitation, whereby information is partially made available to the user, but further access thereto requires acceptance of cookies (including non-essential cookies).[81] For example, a website may place a cookie consent notice directing the user to accept non-essential cookies and should the user not do so, redirect them to another webpage, usually their privacy policy, similarly barring access.[82] A further, and very common, practice among sites that do attempt to simulate compliance with the requirement for obtaining data subjects' consent is the pre-selection or pre-ticking of cookies with no direct option to reject non-essential cookies.[83] Some websites, for example will have all cookie options already pre-ticked but the user needs to manually untick the non-essential cookie options themselves should they not wish to consent thereto.

An even more sketchy technique is the pre-selection of cookie options and third-party legitimate interests which each need to be manually unticked by the user should they similarly not wish to consent to the processing.[84] The number of pre-selected third-party legitimate interests on a cookie request can be quite long and time-consuming, such that users may be driven to a state of so-called cookie or consent fatigue. Consent fatigue generally refers to a condition whereby web user is overwhelmed or desensitised by constant requests for cookie consent such that they end up agreeing to the processing of their personal information even if they do not really intend to grant such consent.[85] Poor configuration of cookie requests such as those described above can exacerbate this condition.

The question therefore arises whether any of the above examples constitute a valid request for consent and whether the consent thereafter obtained is consistent with consent as contemplated under section 1 (and by extension 11 and 12) of the POPIA? Without a need to stretch, the answer to the question above is simple: all but one do not. It is well-established that the POPIA requires a data subject to consent to the processing of personal information and that a responsible party must obtain consent should it wish to collect personal information from third parties. Similarly, it is established that this requirement applies to cookies too. Consent as contemplated by the POPIA, however, is not merely an act of agreeing to something. It must both be an informed agreement which is free from coercion, undue influence or external pressure. In other words, the user must not only be adequately informed of the purpose of the processing but must wilfully agree thereto without a threat of some kind, should they wish not to tender such agreement. It is the duty of the responsible party to ensure that a data subject is provided with complete information necessary for them to make an informed decision (including information about what the responsible party uses personal information for). As Da Veiga *et al.* note, however, South African websites (at least in the context of e-commerce) rarely provide complete information to users in their cookie requests.[86] Even where such information is duly provided, the aspect of voluntariness would operate against many of these sites' cookie requests. For one, the lack of a clear option in certain websites allowing users to choose whether to accept certain cookies means that users are put in a corner as consent for all processing is essentially implied or presumed by access. Such consent cannot logically (or even legally) be interpreted as a voluntary, specific and informed expression of will.

80 *Ibid*.

81 *Ibid*.

82 *Ibid*.

83 Utz *et al.* "(Un)informed Consent" 976.

84 *Ibid*.

85 Utz *et al.* "(Un)informed Consent" 973.

86 Da Veiga *et al.* "Evaluating Data Privacy" 2706–2707.

It may be possible for "consent" of this nature to be informed in circumstances whereby websites do provide complete information, but the absence of an option to decline cookies means that choice as an independent, voluntary decision is entirely obviated. Although consent to processing may be impliedly obtained under the POPIA,[87] it can rarely be the case where there is a clear lack of choice to refuse non-essential cookies. Like websites that impose an access barrier conditioned upon acceptance of non-essential cookies, the lack of a choice to reject such cookies essentially coerces data subjects into an extortionary processing agreement. As such, consent obtained in this manner is something akin to consensus obtained by undue influence. Accordingly, it does not constitute valid consent as contemplated by the POPIA since it is not truly voluntary.

A more challenging scenario is posed by the consent fatigue-inducing practice of pre-ticked cookie requests with no overriding option to reject all non-essential cookies. For one, the user is presented with a choice whether to agree to processing or not. However, the exercise of choice is structurally and deliberately rendered complicated because, as opposed to opting-in, opting-out is not afforded the same ease of execution. Instead, the user must painstakingly go through every pre-ticked cookie option manually in order to tender an effective rejection thereof. In this regard, the user is forced to spend more time trying to metaphorically "get out of the woods" than they would need to, had they simply consented. However, the POPIA and its regulations are silent on this issue. Considering the wording of the POPIA as concerns the meaning of consent, it is difficult to conclude that this type of strategic cookie request manoeuvring is inconsistent. Unlike the GDPR, which is discussed below, the POPIA does not create an obligation for responsible persons to make withdrawal or refusal of consent easy. It also does not require responsible parties to ensure that a cookie consent request be user friendly. Instead, it simply creates a framework that requires them to provide the choice to consent. How they go about doing so is entirely unregulated.

4 COOKIE REGULATION IN THE EUROPEAN UNION

4 1 EU Data Protection Regulations

Following on the heels of the much broader Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 108,[88] adopted by the Council of Europe in 1981, the EU adopted the Directive 95/46/EC, better known as the Data Protection Directive, in 1995. The Data Protection Directive[89] sought to harmonise laws regulating data across the EU and to facilitate the free flow of information between member states.[90] It also sought to balance the

87 For example, where the user has a choice to accept or decline and chooses to ignore the options but continues to access the site, it is logical to presume consent to processing even if not expressly pronounced. The EU position is different from the present authors' view since the European Data Protection Board (EDPB) has indicated that simply scrolling through a website does not amount to consent. In this respect, the authors agree that this cannot amount to consent if an opportunity to exercise effective consent is not provided. However, where users are provided with such a choice and opt to ignore it while using the services provided uninterruptedly, it would seem strange (if not wholly unfair to the responsible party (or controller)) to conclude that the user did not tacitly give consent through continued use. If anything, it is submitted, the difficulty would be in determining the point at which such consent should be implied — see European Data Protection Board (EDPB) *Guidelines 05/2020 on consent under Regulation 2016/679* (2020) 18.

88 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981.

89 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 (Data Protection Directive).

90 Birnhack "The EU Data Protection Directive: An Engine of a Global Regime" 2008 *Computer Law & Security Review* 508 512.

internal market's trade needs with the protection of personal data.[91] However, broad compliance with the Directive was not achieved and there was instead fragmentation in regulations between member states.[92] EU directives, unlike EU regulations, generally state an objective but leaves it up to member states to determine how they go about achieving it.[93] Regulations, on the other hand, apply to member states in their entirety.[94] Consequently, and given the need to enforce broad compliance across all EU member states, the GDPR was adopted in 2016. The GDPR introduced strictly defined and enforceable requirements on personal data collection and tracking. Its scope of application is broad and includes businesses and website operating within the EU and those providers offering services to EU citizens, but not necessarily based there.[95]

The GDPR lays down several principles for data processing which must be complied with by persons responsible for collecting personal data and deciding on the purposes therefor (i.e., the data controller). These principles *inter alia* include processing lawfulness, transparency and fairness, purpose specification and process limitation, data minimisation, data adequacy and security.[96] A data controller is responsible and by extension liable for all personal data processing it conducts or authorises.[97] It must therefore implement effective measures to ensure GDPR compliance and must be able to demonstrate adherence thereto. Compliance measures should reflect the processing's nature, scope, purpose, and risks to individuals' rights and freedoms.[98] Six conditions are set down in Article 6 of the GDPR to inform the lawful processing of personal data. The processing of personal data will be considered lawful when either the data subject has given their consent or if it is necessary for the performance of a contract, compliance with legal obligations, or to protect the vital interests of the data subject or another natural person.[99] Processing will also be lawful if it is essential to the performance of a task in the public interest, or by the legitimate interests of the controller or a third party, unless such interests are overridden by the data subject's rights.[100]

Functioning together with the GDPR is Directive 2002/58/EC better known as the ePrivacy Directive,[101] which complements the now-repealed Data Protection Directive of 1995.[102] It is predominantly in terms of this regulation that cookies are regulated.

4 2 Consent under EU Data Protection Law

The GDPR requirements for valid consent are dealt with in a more extensive manner compared to the POPIA. Article 7(1) of the GDPR requires a controller to demonstrate that a data subject has indeed given valid consent.[103] Consent will be valid if it is *unambiguous* and given *freely*,

91 *Ibid*.

92 Cervi "Why and How Does the EU Rule Global Digital Policy: An Empirical Analysis of EU Regulatory Influence in Data Protection Laws" 2022 *Digital Society* 1 20; see also Chassang "The Impact of the EU General Data Protection Regulation on Scientific Research" 2017 *Ecancermedicalscience* 1 2.

93 Memić *et al. Regulations and Directives—Past, Present, Future* (2023) 5 8.

94 *Ibid*.

95 Article 3 of the GDPR.

96 *Ibid* art 5.

97 *Ibid* Recital 79.

98 *Ibid*.

99 *Ibid* art 6(1).

100 *Ibid*.

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

102 Article 1(2) and 2 of ePrivacy Directive.

103 Article 7(1) of the GDPR.

specifically, and with the user being *properly informed*.[104] The controller is further enjoined to ensure that where consent is given by written declaration concerning other matters, the former must be separate from the other matters, be easy to understand for the data subject, and be written in clear and plain language.[105] According to Recital 43, consent will be deemed not to have been freely given if the data subject is not given the opportunity to separately consent to distinct data processing operations. Even if processing multiple types of personal data may be appropriate in the circumstances, consent will still not be freely given if the data subject is not given the option to consent to each operation individually.[106]

The data subject is entitled to withdraw consent at any time and the process of withdrawing consent must not be more cumbersome than the giving thereof.[107] However, like the POPIA, withdrawal does not affect prior processing of personal data.[108] Another aspect of valid consent under the GDPR concerns the issue of consent "bundling". In essence, bundling occurs when the user is required to consent to the processing of personal data for uses that are not necessary for the performance of the service sought. In other words, the controller bundles together non-essential requests with essential requests such that the user, in accepting the latter, also automatically consents to the former, which serves purposes that are not relevant or necessary to the service sought. Article 7(4) prohibits bundling, providing that when determining if consent is freely given, regard must be had to the question whether the performance of a contract is incumbent upon the data subject giving "consent to the processing of personal data that is not necessary for the performance of that contract."[109] In other words, where the data subject is required to consent to processing, such processing must be necessary for the performance or provision of that service. A controller can thus not refuse to provide a service to a data subject should they not agree to processing of irrelevant data.

The explanation given in the GDPR regarding the conditions for consent is quite revealing. Recital 32 of the GDPR expounds on what necessarily would constitute valid consent and indicates that the validity of a data subject's consent is conditioned upon it being "a clear affirmative act" showing that a data subject agrees to the processing of their personal data, irrespective of whether this consent is given by written or oral statement, by electronic means or actions like the ticking of a box and adjustment of technical settings to that effect.[110] It is important to note that when consent is requested electronically, the requestor's information needs to be clear, concise, and must not unnecessarily interfere with the user's experience of the service.[111] The recital explicitly indicates that it is not possible to imply or presume consent. Where the controller does not tender a request for consent, or pre-selects options giving consent to processing on behalf of the data subject, consent is not present.[112] Simply, there can be no consent if a data subject does not individually choose the data processing operations for which they are consenting. Put differently, consent to processing of personal data can only be valid if it is *active*.

104 *Ibid* art 4(11) [emphasis added].

105 *Ibid* art 7(2).

106 *Ibid* Recital 43.

107 *Ibid* art 7(3).

108 *Ibid.*

109 *Ibid* art 7(4).

110 *Ibid* Recital 32.

111 *Ibid*.

112 *Ibid*.

4 3 Cookies under EU Data Protection Regulations

Within the context of cookies, Article 5(3) of the ePrivacy Directive (much like the GDPR) requires that "electronic communications networks" used to store and access information on the data subject's terminal equipment or computer device be allowed only on condition that the data subject is clearly and comprehensively informed about the purposes of the processing "in accordance with Directive 95/46/EC, … and is offered the right to refuse such processing by the data controller."[113] This condition does not apply to communication that is strictly necessary, however. Unlike the GDPR, the data protected under the ePrivacy Directive need not constitute personal information to be protected. The ePrivacy Directive considers all information, including personal information, stored on a data subject's terminal equipment as falling within the "private sphere" and therefore protected under the European Convention for the Protection of Human Rights and Fundamental Freedoms.[114] Despite giving cognisance to the benefit and use of cookies in Recital 25, the Directive notes that devices such as cookies should be allowed "only for legitimate purposes, with the knowledge of the users concerned."[115] It further clarifies that when informing users about the purposes of cookies, controllers must ensure that the information thus given must be precise and clear and the method by which it is conveyed should also be "as user-friendly as possible."[116] Interestingly, the recital further notes that acceptance of cookie installation and storage can be used as a precondition for accessing a service, provided that the cookies are used also for a "legitimate purpose."[117] What constitutes a legitimate purpose is not explicitly expounded upon in the Directive. However, the wording of Article 5(3) of the ePrivacy Directive, read together with Article 7(4) of the GDPR suggests that the installation and storage of cookies and similar technologies is not precluded, provided that it is for the

> sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.[118]

It may, accordingly, be inferred that for a purpose to be deemed legitimate in terms of the proviso under Article 5(3), it must be indispensable to the data subject's experience of the service sought, rather than merely serving the interests of the service provider, such as for purposes of analytics or targeted advertising. In such cases, clear and informed consent would need to be obtained before any storage or access can take place.

4 4 On Cookie Compliance

One will recall the discussion above concerning the various methods by which cookie consent requests may be presented to end-users. Without needing to resort to strained interpretations, none of the methods of requesting consent discussed, can be considered appropriate under the GDPR. This is because they either would fail for want of consent as such, active consent or due to consent bundling. The treatment of pre-selected cookie consent options, whether for legitimate interests of the controller or third parties and checkboxes on cookie consent requests, all of which would be valid under the POPIA, is quite different under the GDPR. As discussed above, the POPIA merely requires that consent be voluntary, specific and informed. As long as a responsible party furnishes the data subject with the full information specifically and clearly

113 Article 5(3) of the ePrivacy Directive; see also generally ss 6 and 7 of GDPR.

114 Recital 24 of the ePrivacy Directive.

115 *Ibid* Recital 25.

116 *Ibid*.

117 *Ibid*.

118 *Ibid* art 5(3).

addressing each processing purpose, and the same is imbued with a semblance of choice, such a cookie consent request would be valid.

The questions of pre-selection of options, separate consent, active consent and bundling under the ePrivacy Directive and Data Protection Directive (read with the GDPR) were each addressed by the Court of Justice of the European Union (CJEU) in *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände* (*Planet49*).[119] The case concerned a prospective participant in a Planet49-organised promotional lottery, who was confronted with a request for consent that included two checkboxes.[120] The first checkbox which was unticked by default, required the user to consent to "sponsors and cooperation partners" sending telephonic or email/SMS marketing communication relating to "offers from their respective commercial sector."[121] The second checkbox was pre-ticked and authorised the installation of cookies to enable tracking for targeted advertising.[122] In order to participate in the promotional lottery, participants were required to accept at least the first checkbox.

The first checkbox, although not forming part of the referral, was still considered by the CJEU for compliance with the prohibition against bundling. The court noted that a competent court was enjoined, taking into account the Article 7(4) prohibition on bundling, to determine whether the processing of personal data was necessary in order to provide the service sought by the data subject.[123] According to the court, inherent to participating in the Planet49 lottery was the requirement to sell personal data to the lottery's sponsors for their marketing communication purposes.[124] In this regard, the first checkbox was deemed compliant as the provision of such data "constitute[d] the main obligation of the user in order to participate in the lottery."[125]

The second, pre-ticked, checkbox allowing for the installation and gaining access of cookies on the user's terminal equipment, however, was not met with the same outcome. As it concerned cookies, the second checkbox fell within the ambit of Article 5(3) of the ePrivacy Directive.[126] The CJEU, considering whether or not the pre-ticking of the option constituted valid consent, opined that to require a data subject to actively untick a checkbox to indicate their non-consent could not meet the requirement for active consent.[127] If anything, it was impossible to tell if the user had given any informed consent at all.[128] One may reason that the court's position is due to the fact that the action of unticking is generally passive in nature since it only happens in the event of the data subject actively intervening to *refuse* and *not to give* consent. In the ordinary course, a data subject simply confirming acceptance of conditions to receive a service will, by implication, be consenting to the cookie installation without having actively, affirmatively and deliberately given informed consent.[129] Consent obtained in this manner would instead have been presumed on their behalf by the controller and can, accordingly, neither be considered voluntary, affirmative nor informed.

---

119 *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e V* Case C-673/17.

120 *Ibid* para 1–3.

121 *Ibid* para 24.

122 *Planet49* para 25.

123 *Planet49* para 99.

124 *Ibid*.

125 *Ibid*.

126 Read with art 2(f) of ePrivacy Directive, art 2(h) of the Data Protection Directive and art 4(11) of the GDPR.

127 *Planet49* para 88.

128 *Ibid*.

129 In explaining what is meant by a "clear affirmative act", the EDPB explains that the data subjects need to have taken a deliberate action of consent to said processing operation — EDPB *Guidelines 05/2020* 18.

The court found the converse,[130] however, to constitute valid and active informed consent.[131]

Another issue concerning the pre-ticking of the second checkbox was that it failed to give the data subject the ability to exercise separate consent.[132] It should be recalled that consent must not only be freely given and informed, but should also be specific. This is a feature of the definition under the GDPR and the ePrivacy Directive.[133] As discussed above, the GDPR requires that specific consent requests be presented separate from other distinct matters.[134] *In casu*, the pre-ticking rendered the separate act of accepting conditions for partaking in the lottery and that of consenting to the installation and gaining access of cookies, into a single composite act.[135] It thus failed, in essence, to provide sufficient separation between two individually distinct decisions. Planet49's case was not helped by the fact that the first checkbox was the only essential requirement to participate in the lottery, but the users were also not informed that it was not necessary to accept the second checkbox.[136] According to the CJEU, the second checkbox violated the provisions of Article 5(3) and 2(f) of the ePrivacy Directive as it could not be said that a data subject would be "in a position to freely give his separate consent to the storing of information or the gaining of access to information already stored, in his terminal equipment."[137]

5 CONCLUSIONS

From the foregoing, the difference between the POPIA and the GPDR is evident. With regard to the regulation of methods of obtaining the requisite consent necessary for the processing of personal information, the POPIA seems to adopt a much more laissez-faire approach than the GDPR. Under South African legislation, the responsible parties are given greater leeway to decide how to present cookie consent requests. In this regard, responsible parties are free to decide whether to make cookie clickwraps easy and user-friendly or complicated, time-consuming and taxing on the end user. For as long as the POPIA requirement for consent is complied with, it appears that the legislature could not be concerned about the ease with which user consent may be denied or withdrawn. The GDPR, on the other hand, presents the stark opposite of the POPIA. Rather than opening the door for controllers to make decisions about presentation and presumption of consent on cookie requests, the EU legislation explicitly delineates each aspect thereof. As a result, a data subject under the GDPR is not only liberated from the burden of poorly configured cookie consent requests but is also enabled to exercise true consent. The same, it is ultimately submitted, cannot be said of the South African data subject.

With the above conclusions in mind, it is recommended that the Information Regulator issue guidelines regarding the proper implementation of website cookie requests. The aim of these guidelines should be to ensure that cookie requests are made to users in a clear and concise manner that enables them either to accept or reject multiple requests at once should they wish to do so. While an amendment to the POPIA to this effect would certainly add more certainty, the aforementioned proposal is also adequate and can be supported within the meaning of consent under section 1 of the POPIA.

130 That is, where the data subject has the option to actively tick the checkbox.

131 *Planet49* para 88.

132 As required under art 7(2) of the GDPR.

133 The latter's definition is sourced from art 2(h) of the Data Protection Directive.

134 *Ibid*.

135 *Planet49* para 89.

136 *Ibid* para 89–92.

137 *Ibid* para 90.