Strathmore Law Review (SLR)
eISSN: 2414-8164 – Volume 7, Issue 1 (2022) p.127-159
https:doi.org/10.52907/slr.v7i1.194

Safeguarding Personal Data: Meta Consent as a Remedy to Section 28(2)(c) of Kenya's Data Protection Act

*Wanditi Gathumbi**

Abstract

Biometric identity systems have been adopted in the Global South, following the Global North's lead. The greatest discrepancy, however, is the existence of legal frameworks that govern the use, storage and processing of the data collected. The Kenyan government's roll-out of the Huduma Namba registration exercise in April 2019 with no existing data protection law in Kenya exemplifies this. Thereafter, Parliament passed the Data Protection Act. Unfortunately, parts of this law are not keen enough to protect personal data. Deviating from the requirement for personal data to be directly collected from the data subject, section 28(2)(c) of the referenced Act permits indirect collection of personal data from a source other than the data subject themselves. Relying on desk-based research and using the Huduma Namba exercise as a case study, this paper examines this permission and the imminent danger it poses to privacy of the personal data of Kenyans. Finding that section 28(2)(c) exposes personal data to the privacy violations of secondary use and exclusion threatens the right to privacy, this research suggests that the meta consent model as embraced by the healthcare sector emerges as a feasible solution. This model allows data subjects to determine their consent preferences i.e., how and when they wish their consent to be sought for further collection and use, at the point of primary collection of personal data. Additionally, this paper recommends that the model should be embraced by the judiciary in its adjudication of matters and finally, that an amendment incorporating the solution should be made.

Keywords: *Privacy, Personal Data, Indirect Collection, Data Protection, Secondary Use, Exclusion, Meta Consent*

* The author is an LLB graduate from Strathmore Law School who is passionate about privacy and data protection research from an African perspective. She wishes to extend her deepest gratitude to her family and friends for supporting this endeavour, but most especially to Mr Collins Okoh and Mr Arnold Nciko for their resolute belief in the author.

Table of Contents

I. Introduction

The trend of using biometric identity systems by governments in the Global North is currently being adopted in the Global South.[1] A study conducted on the use of biometric systems showed a 37 percent estimated growth rate of the biometric industry in Africa between 2005 and 2010, making it the region with the most rapid growth in that period.[2] Subsequently, research on the application of biometric identification technologies in developing countries identified 75 cases in sub-Saharan Africa where the systems are functioning to provide identification, democratic participation and delivery of services.[3] The greatest disparity, however, is the existence of legal frameworks, guidelines and laws that check the use, storage and handling of the data collected. According to Privacy International, as of March 2020, only 24 out of 53 African countries had enacted legislation and regulations oriented towards the protection of data.[4] Even more problematic, these laws tend to be lifted from existing legislation in the West such as the European General Data Protection Regulation (hereafter GDPR) effectively failing to take the local context into account.[5] This transplant is in some ways an undesirable approach to legislating due to the glaringly different contextual circumstances: where one is resource-rich and the other is resource-deficient and developing.

While the Global North seems to have a good handle on data protection, as exemplified by the GDPR being considered as the 'new gold standard',[6] countries in the Global South seem to be in over their heads, facing the uphill task of meeting the internationally accepted standards. An example of this is the GDPR

---

1 Gelb A and Clark J, 'Identification for development: The biometrics revolution' Centre for Global Development, Working Paper 315, 2013, 2 -<Identification for Development: The Biometrics Revolution (ethz.ch)> on 3 January 2021.

2 Gelb A and Clark J, 'Identification for development: The biometrics revolution' Centre for Global Development, Working Paper 315, 2013, 66 -<Identification for Development: The Biometrics Revolution (ethz.ch)> on 3 January 2021.

3 Gelb A and Clark J, 'Identification for development: The biometrics revolution' Centre for Global Development, Working Paper 315, 2013, 20 -<Identification for Development: The Biometrics Revolution (ethz.ch)> on 3 January 2021.

4 '2020 is a crucial year to fight for data protection in Africa' Privacy International, 3 March 2020 -<2020 is a crucial year to fight for data protection in Africa | Privacy International> on 3 January 2021.

5 '2020 is a crucial year to fight for data protection in Africa' Privacy International, 3 March 2020 -<2020 is a crucial year to fight for data protection in Africa | Privacy International> on 3 January 2021.

6 'The state of data protection rules around the world: A briefing for consumer organisations' Consumers International, 25 May 2018 < gdpr-briefing.pdf (consumersinternational.org)> on 3 January 2021.

providing for indirect collection of data vide another source subject to different levels of consent.[7] Kenya equally makes a similar provision in section 28(2)(c) of the Data Protection Act (hereinafter referred to as the DPA). It allows for direct collection of data making an exception for indirect collection of data where the data subject had previously consented to the collection of the same from another source.[8] This, creating a major problem for individuals' privacy rights, is the main focus of the paper.

Data protection in Kenya took centre stage when the government rolled out the Huduma Namba registration in April 2019.[9] The exercise would see the government collect and aggregate inordinate amounts of personal data of its citizens in the newly introduced biometric system, National Integrated Identity Management Scheme (NIIMS).[10] Legally, the government was ill-equipped to be carrying out such a grand mass registration scheme with no existing harmonised data protection law in Kenya. Albeit the little-debated Data Protection Bill, 2013, this left all questions on the safety and privacy of personal data unanswered.[11]

In response, the High Court issued an interim ruling which *inter alia* put a caveat on the collection of biometric and personal data. Per the ruling, collection could only be done under the regulation of an appropriate legislative framework protecting fundamental rights.[12] The most fundamental right considered was the right to privacy. Forging ahead, the government relied on data protection regulation scattered in different pieces of legislation that were hardly satisfactory to safeguard fundamental rights.[13] Privacy International's report, the *State of Privacy in Kenya*, notes this lack of a specific data protection law at the time.[14] The court noted this when it concurred with the petitioner that the legal framework

---

7 Article 13(3), *General Data Protection Regulation* (2016/ 679 of the European Parliament).

8 Section 28(2)(c), *Data Protection Act* (No. 24 of 2019).

9 Houghton I, 'It is critical we get it right on Huduma Namba registration' The Standard, 20 July 2019 -<It is critical we get it right on Huduma Namba registration - The Standard (standardmedia.co.ke)> on 5 January 2021.

10 Houghton I, 'It is critical we get it right on Huduma Namba registration' The Standard, 20 July 2019 -<It is critical we get it right on Huduma Namba registration - The Standard (standardmedia.co.ke)> on 5 January 2021.

11 *Nubian Rights Forum & 2 others v Attorney General & 6 others and Child Welfare Society & 8 others* (2020) eKLR.

12 *Nubian Rights Forum & 2 others v Attorney General & 6 others and Child Welfare Society & 8 others* (2020) eKLR.

13 The Children's Act (No. 8 of 2001), The Elections Act (No. 24 of 2011), The Registration of Persons Act (Cap. 107), Kenya Information and Communications Act (Cap. 411A) and the Private Security Regulation Act (No. 13 of 2016) among others.

14 Privacy International and National Coalition of Human Rights Defenders-Kenya, *The State of Privacy in Kenya,* 2019.

on the functioning of NIIMS was '[inadequate and] poses a risk to the security of data'.[15] This left the personal data collected at risk of privacy violations which have been categorised into four groups: information processing, information collection, information dissemination and invasion.[16]

This exercise exposed personal data to the privacy problems of secondary use and exclusion, extant within the information processing category. Secondary use is the further use of data for a motive that is unrelated to the original motive that data was first collected for.[17] Exclusion happens when the data subject is precluded from knowing which of their personal data is held and from having a say in how their data is used after it is surrendered to the data controllers.[18]

Shortly after, Parliament passed the Data Protection Act, 2019. Its purpose was to operationalise the constitutionally afforded right to privacy.[19] Constitutionally, the right to privacy grants people the protection against 'information relating to their family or private affairs unnecessarily required or revealed'.[20] This right safeguards the autonomous and private sphere of the person that is to be free from unsolicited interference by the State or other individuals.[21] It affords people the opportunity to have reasonable control over how they are presented to others[22] and how their personal information is used.[23] The importance of this protection is multipronged as there are not only many elaborations of its importance, but its importance also serves to exhibit why it should be protected. Summarily, the right to privacy is important because (1) it is necessary for people's well-being as it allows them to exercise their autonomy over their proximity to others in society.[24] This distance allows them to fully express themselves far from the watchful gaze of outsiders.[25] (2) The separation it creates allows people to 'maintain a system of different relationships with

---

15 *Nubian Rights Forum & 2 others v Attorney General & 6 others and Child Welfare Society & 8 others* (2020) eKLR.

16 Solove DJ, '"I've got nothing to hide" and other misunderstandings of privacy', 44(745) San Diego Law Review, 2007, 758.

17 Solove DJ, 'A taxonomy of privacy', 154(3) *University of Pennsylvania Law Review*, 2006, 521.

18 Solove DJ, 'A taxonomy of privacy', 490.

19 *Data Protection Act* (No. 24 of 2019).

20 Article 31(c), *The Constitution of Kenya* (2010).

21 Privacy International and the National Coalition of Human Rights Defenders in Kenya, *The right to privacy in Kenya*, 2015, 2 - https://privacyinternational.org/sites/default/files/2017-12/UPR%20Kenya.pdf on 10 May 2022.

22 Marmor A, 'What is the right to privacy' 43(1) *Philosophy & Public Affairs*, 2015, 13.

23 Moore A, 'Defining privacy' 39 *Journal of Social Philosophy* 3, 2008, 414.

24 Marmor A, 'What is the right to privacy', 10 -11.

25 Diggelmann O and Cleis MN, 'How the right to privacy became a human right', 14 *Human Rights Law Review*, 2014, 458.

different people'[26] as the nature of a relationship determines a person's behaviour. (3) It also serves as a foundation for the enjoyment of other rights, particularly the right to freedom of expression, religion, and association. The opportunity to exercise these rights rests on the foundation and protection of the right to privacy.[27]

Inasmuch as the enactment of the DPA has served to illuminate the murky waters of data security, it must be noted that it suffers from shortcomings. Aiming at the protection of individual privacy and regulating the processing of personal data, inter alia,[28] it falls short on fulfilling these goals as this article will illustrate. Particularly, this paper focuses on the DPA's legislation on indirect collection of personal data in section 28(2). It permits indirect collection in six different instances without seeking further consent of the data subject as a proviso to section 28(1).[29] These include where the data is collected from a public record,[30] where the data is collected from another source that the data subject had consented to[31] and where the collection would not be detrimental to the data subjects' interests.[32] This exposes collected personal data to the privacy violations of secondary use and exclusion.

Consequently, the objective of this article is to exhibit that the permission granted to data controllers enabling them to indirectly collect personal data in section 28(2)(c) of the DPA impairs the right to privacy. Ergo, the central claim of this article is that section 28(2)(c) leaves personal data susceptible to the privacy violations of secondary use and exclusion thus threatening the right to privacy.

Part I of this paper forms the introduction, providing background information on the present status of data protection of Kenya and its connection to the right to privacy. Against this background, Part II introduces the taxonomy of privacy as a grounding framework for this paper. Part III investigates whether section 28(2)(c) contravenes the right to privacy and its failure to protect personal data from the privacy violations of secondary use and exclusion. Part IV juxtaposes the framework's perception of privacy to the one adopted in drafting

---

26 Rachels J, 'Why privacy is important', 4 *Philosophy & Public Affair*s 4, 1975, 330.

27 National Coalition of Human Rights Defender-Kenya (NCHRD-K), the Kenya Legal & Ethical Issues Network on HIV and AIDS (KELIN), Paradigm Initiative, and Privacy International, *The right to privacy in Kenya*, 2019, 3.

28 Section 3(a) and 3(c), *Data Protection Act* (No. 24 of 2019).

29 Section 28(2), *Data Protection Act* (No. 24 of 2019).

30 Section 28(2)(a), *Data Protection Act* (No. 24 of 2019).

31 Section 28(2)(c), *Data Protection Act* (No. 24 of 2019).

32 Section 28(2)(e), *Data Protection Act* (No. 24 of 2019).

section 28(2)(c) of the DPA. Part V considers a possible solution to remedy the problem of insecurity of personal data under Section 28(2)(c). Finally, Part VI considers the feasibility of implementing the proposed solution in the Kenya's data protection sphere and Part VII concludes the paper.

II. Taxonomy of Privacy

Daniel J Solove's theory is grounded on the elusive nature of privacy that has seen it characterised as abstract.[33] This has resulted in a consistent inability of scholars to ascribe a befitting definition to privacy. Consequently, this narrative of privacy is so prevalent that it prompted Kim Scheppele to note that privacy suffers from 'an embarrassment of meanings'.[34] This lack of a comprehensive definition creates a curious problem of the inability of lawmakers to create policies and laws that adequately protect against privacy harms and leaves judges wrestling to adjudicate over cases.[35]

In a bid to avoid making the same mistakes, Solove resorts to conceptualising privacy as a 'set of family resemblances' contrasting the traditional method of defining by pinpointing the essence of the thing.[36] He does this by recognising that privacy is a plural concept and not a singular one, drawing from Ludwig Wittgenstein's argument that some concepts have 'a complicated network of similarities overlapping and criss-crossing: sometimes overall similarities, sometimes similarities of detail'.[37] Privacy is one of such concepts as it covers a conglomeration of things.[38] Conceptualising privacy singularly presupposes that privacy has a one essence yet, as Solove exhibits, this is not the case. The dangers of defining privacy singularly are that different violations are conflated and the problem at hand may not be recognised entirely.[39]

The taxonomy takes a bottom-up approach to conceptualising privacy unlike the widespread approach that defines privacy singularly.[40] Thus, Solove

---

33 Solove DJ, Conceptualizing privacy, 90 *California Law Review* 1089, 2002, 1128.

34 Scheppele KL, *Legal secrets: Equality and efficiency in the common law,* University of Chicago Press, Chicago, 1988, 184-185.

35 Solove DJ, 'A taxonomy of privacy', 480.

36 Solove DJ, "'I've got nothing to hide" and other misunderstandings of privacy' 44 *San Diego Law Review* 4, 2007, 756.

37 Wittgenstein L, *Philosophical investigations*, 3rd ed, Pearson, London, 2001, 65.

38 Solove DJ, *Conceptualizing privacy,* 1128.

39 Solove DJ, 'A taxonomy of privacy', 481 - 482.

40 Massey AK and Antón AI, 'A requirements-based comparison of privacy taxonomies', Requirements in Engineering and Law, Barcelona, 9 September 2008, 3.

creates a taxonomy of privacy where he contemplates a myriad of harmful activities that invade the privacy of an individual.[41] Eventually these activities culminate in privacy problems which he compacts into four categories. Namely, information collection, information processing, information dissemination, and invasion. Within these groups, he sets out different activities that constitute privacy violations, including exclusion, surveillance, insecurity, and secondary use, among others.[42]

The assembling of the taxonomy is systematic as it moves from the data subject outwards. To better grasp the taxonomy's categorisation of privacy problems, the author briefly elaborates on each category and draws connections to the Kenyan context.

Information collection is the process of accumulating information from the data subject. This may be exemplified by the Huduma Namba exercise where the Kenyans were called to surrender their personal information to the government.[43] This aggregation of personal data in a central database creates opportunity for the government to engage in surveillance of citizens. The Kenyan government has done this before with the National Intelligence Service having direct access to telecommunications networks operating in the country for surveillance purposes.[44] On the other hand, information processing makes use of the data collected, alters it, and stores it.[45] The data harvesting and mining scandal by Cambridge Analytica to socially engineer the votes of Kenyans and guarantee the success of the Jubilee coalition in the 2013 and 2017 Kenyan presidential elections illustrates the information processing situation in Kenya.[46]

---

41 Solove DJ, 'Understanding privacy' The George Washington University Law School, Public Law and Theory Working Paper Number 420, 2008, 10 -11 <https://poseidon01.ssrn.com/delivery.php?ID= 261087081122064118116070106081098071052087053042027060078071082 126091094081027009022019114028045009056121075004112005109014021098080071048000104066093119019106011051008075106092102100064119104124 028112087108075001103070120091126003004089008 112006071&EXT=pdf_>- on 12 June 2020.

42 Solove DJ, 'Understanding privacy', 10.

43 Houghton I, 'It is critical we get it right on Huduma Namba registration' The Standard, 20 July 2019 -<It is critical we get it right on Huduma Namba registration - The Standard (standardmedia.co.ke) on 5 January 2021.

44 Privacy International and National Coalition of Human Rights Defenders-Kenya, *The State of Privacy in Kenya,* 2019.

45 Massey AK and Antón AI, 'A requirements-based comparison of privacy taxonomies', 3.

46 Warah R, 'Cambridge Analytica and the 2017 elections: Why has the Kenyan media remained silent?' The Elephant, 9 August 2019 -< RASNA WARAH - Cambridge Analytica and the 2017 Elections: Why Has the Kenyan Media Remained Silent? | The Elephant> on 3 April 2022.

Information dissemination is concerned with the propagation of information or the 'threat to do so'.[47] Once more, the author refers to the Huduma Namba debacle to locate this phenomenon in the Kenyan context. Disturbingly, the Huduma Namba data capture-form included a declaration that the Kenyan government would thereby be permitted to disclose the information to 'authorised Government agency/agencies'.[48] This ultimately presents an occasion for the collected information to be disclosed within the government. The fourth category, invasion, is the interference with personal and private affairs. It need not always pertain to personal information; however, it mostly does.[49] The two privacy violations that the author identifies as possible consequences of section 28(2)(c) which are secondary use and exclusion fall within the information processing category according to Solove.[50]

Categorising these activities is done to identify the problems and elaborate on their problematic nature thereby curing the abstract conceptualisation of privacy.[51] In turn, this advances the legal system's understanding of the concept of privacy and Solove hopes it will eventually ameliorate the legislation of privacy.[52]

The taxonomy exhibits structural problems that are likely to manifest future harm to the data subjects in its categorisation of harmful activities. The first of such problems is that these activities intensify the peril that harm will occur to the personal data.[53] Solove acknowledges that where personal information is available, the risk of harm being done to a data subject is significantly increased. He references harms such as 'identity theft [and] fraud'.[54] Whereas the second problem is that the activities shift the balance of power from the data subject to the data controller, socially and institutionally, commonly referred to as the chilling effect.[55] This is a phenomenon where as a result of state action, a data subject is deterred from exercising their rights in fear of formal state action against them and the power wielded over them.[56] In this case, the state action

47 Solove DJ, 'A taxonomy of privacy', 491.

48 See the Huduma Namba Digital capture form here form hn 24-Data Capture Tools-14-5-2019 (hudumanamba.go.ke).

49 Solove DJ, 'A taxonomy of privacy', 491.

50 Solove DJ, 'A taxonomy of privacy', 490.

51 Solove DJ, 'Understanding privacy', 2.

52 Massey AK and Antón AI, 'A requirements-based comparison of privacy taxonomies', 3.

53 Solove DJ, 'A taxonomy of privacy', 487- 488.

54 Solove DJ, 'A taxonomy of privacy', 488.

55 Solove DJ, 'A taxonomy of privacy', 487.

56 Youn M, 'The chilling effect and private action' 66(5) *Vanderbilt Law Review,* 1481-1482.

would be indirect collection of personal data as permitted by section 28(2) of the DPA.

Far from the ingenuity of the taxonomy of privacy in shedding light on the elusive concept that is privacy, it may be critiqued as not being specific enough to explain how the activities come to be included in the taxonomy. Solove's mission to move away from the strict definition of privacy as a singular concept but instead create a framework for understanding privacy is not lost on the author. In his effort to do so, he steers the conversation in a plural direction.[57] His categorisation of privacy problems into taxonomical groups is designed that it may encompass a great number of activities. However, the criteria that Solove relies on to determine what activity counts as a privacy problem may be considered problematic. His criteria consist of privacy problems that are widely recognised in society in cases, law, constitutions and other sources.[58] Problematically, this presents a challenge for the inclusion of new harmful activities that have not yet been widely recognised as privacy problems in society. An example of a new activity is the publishing and sharing of personal data shared by social media platforms users with third parties for advertising purposes.[59] Conversely, the challenge of excluding harms that are recognised as privacy harms also presents itself.[60] Ryan Calo attributes this problem to the lack of a limiting principle in the taxonomy.[61]

Nonetheless, the author finds that the taxonomy is most appropriate for this study. Accordingly, this concept best buttresses this paper as it comprehensively theorises secondary use and exclusion under the category information processing: privacy violations that may occur under section 28(2)(c). It clearly elucidates and conceptualises the abstract concept of privacy thus exemplifying the misinterpretation of privacy in drafting section 28(2)(c). Moreover, it exhibits how the permissions granted to data controllers contravene the right to privacy in Article 31(c) of the Constitution by contemplating the dangers of indirect collection that often result in secondary use and exclusion. Crucially, it also demonstrates how these violations transgress the data subject's privacy. Whereas this paper aims to uncover the insecurity personal data is exposed to by section

57 Solove D, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy', 760.

58 Solove DJ, 'Understanding privacy', 172.

59 Beigi G and Liu H, 'Identifying novel privacy issues of online users on social media platforms', ACM SIGWEB Newsletter,19 February 2019 -<"Identifying novel privacy issues of online users on social media platforms" by Ghazaleh Beigi and Huan Liu with Martin Vesely as coordinator | ACM SIGWEB Newsletter> accessed on 6 June 2022.

60 Calo RM, 'The boundaries of privacy harm' 86(3) *Indiana Law Journal,* 2011, 1141 - 1142.

61 Calo RM, 'The boundaries of privacy harm' 1142.

28(2)(c), this conceptual framework's categorisation and conceptualisation of the privacy violations that attach to indirect collection provides a reference point.

III. Privacy from Kenya's perspective

Understanding the concept of privacy generally and more pointedly from the Kenyan perspective is central to uncovering the shortcomings of section 28(2)(c) of the DPA, which are discussed later. Therefore, this part of the article sets out to establish the concept and exhibit the wrongful perception of privacy adopted by legislators in drafting the DPA that ultimately culminates in the contentious provision.

i. The concept of privacy

The origin of legal protection for the right to privacy is rooted in Louis Brandeis' and Samuel Warren's article, 'The Right to Privacy'. In this article, they submitted that privacy is the 'right to be let alone'.[62] The pair did not create the right to privacy, they merely advocated for the inclusion of a specific protection that would afford an adequate legal remedy bearing in mind the increasingly perverse invasions of privacy at the time; a problem that has only been exacerbated with time. Previously, the protection afforded to privacy under the common law was the right of an individual to control the extent of access to their 'thoughts, sentiments and emotions'[63] by others. This right was founded on other existing rights and protections and not on privacy itself, making it deficient.[64]

Initially, the protection afforded to the subject matter of privacy was grounded on the concept of breach of contract and abuses of trust or confidence.[65] For this protection to accrue, a relationship between the owner of the private information and the person with whom the information was shared had to exist. Trust or confidence were implied as the grounds upon which the private information was shared. On the other hand, a contract between the two individuals implied that confidentiality would attach to any communication of private matters. The implication of this was that protection would not extend to scenarios where a stranger was surreptitiously in possession of

62 Brandeis LD and Warren SD, 'The right to privacy' 4(5) *Harvard Law Review*, 1890, 205.

63 Brandeis LD and Warren SD, 'The right to privacy', 198.

64 Brandeis LD and Warren SD, 'The right to privacy', 213.

65 Brandeis LD and Warren SD, 'The right to privacy', 207.

private information.[66] Therefore, this position would not adequately protect an individual's privacy as intrusions from strangers were becoming rampant. When it became evident that this foundation was deficient, the right to property in confidential information was then elected as a ground for protection. However, this position required the right to property to be understood in its 'widest and extended sense'.[67] This is because the object and purpose of the right to property at the time only extended to protect corporeal chattels.[68]

Brandeis and Warren understood that privacy possessed inherent value outside the foundations considered above. Therefore, they propounded that privacy required its own protection that was not buttressed on other rights and protections to aptly protect individuals from invasions into the private sphere of their lives. Understanding privacy as individual control over personal information, they found that the right to privacy should allow an individual to have autonomy over their personal information that may be shared publicly and that which should remain private.[69] In the same vein, from a control and use perspective, privacy provides control over access and use of an individual's personal information. Privacy rights give individuals the exclusive right to use and control their personal information – to the exclusion of others.[70]

Reflecting on the above conceptions of the right to privacy leads the paper to Solove's theorisation of the concept of privacy. His perspective, as discussed in section II, is preferred in contrast to the definition of privacy considered above that prioritises locating a singular common factor to which they reduce privacy.

According to Solove, privacy takes on a plural character espousing various problems which are related.[71] The rationale behind theorising the taxonomy of privacy is to provide a clear framework of the privacy problems that exist to better safeguard privacy. Solove's conceptualisation of privacy is founded on the fact that the concept of privacy has inherent social value. In fact, he contends that privacy is an 'internal dimension of society'.[72] The social value of privacy, or even more clearly the societal value of privacy takes the importance of preserving privacy for not only the individual but also the society into

66 Brandeis LD and Warren SD, 'The right to privacy', 211.

67 Brandeis LD and Warren SD, 'The right to privacy', 211.

68 Berle AA, 'Production, property and revolution' 65(1) *Columbia Law Review,* 1965, 4.

69 Glancy DJ, 'The invention of the right to privacy' 21(1) *Arizona Law Review*, 1979, 38.

70 Moore A, 'Defining privacy' 414.

71 Solove DJ, 'The meaning and value of privacy' in Roessler B and Mokrosinska D (eds), *The social dimensions of privacy: Interdisciplinary perspective*, Cambridge University Press, 2015, 80.

72 Solove DJ, 'The meaning and value of privacy', 80.

account. This is achieved by recognising that privacy functions as a common good in society fostering values such as autonomy, intellectual development and facilitating socialising.[73] However, privacy is often viewed as an individual right and consequently, it is undervalued and not safeguarded satisfactorily. Perceiving privacy as such guarantees its failure when balanced against social rights such as the right to information, effectively ensuring that privacy does not receive the protection it deserves.[74] However, John Dewey presents a utilitarian perspective propounding that the value of individual rights is founded on 'the contribution they make to the welfare of the community'.[75] Ergo, privacy must not only be protected for its individual value but also for its contribution to the welfare of the community. Valuing privacy as such allows for sufficient protections to be put in place that limit the state's exercise of power effectively preventing privacy violations such as exclusion and secondary use.

ii. Privacy: A Kenyan perspective

As Kenya emancipated itself from the throes of colonialism, the 1963 Constitution of Kenya was promulgated. The independence constitution's inclusion of the right to privacy extended to a person's home and other property.[76] Notably, the scope of protection did not explicitly extend to personal information. However, an understanding of personal information as property[77] could draw the inference that it would thereby be safeguarded under the ambit of 'other property'.[78]

Contrastingly, some scholars have expressed disdain at the 'propertisation' of personal information precisely because of the alienability right that attaches to property.[79] This has the potential to grossly limit an individual's control over their personal information as upon exercise of the alienability right the individual cannot restrict the purposes for which their data is used.[80] Consequently, this has

---

73 Hughes, K, The social value of privacy, the value of privacy to society and human rights discourse' in Roessler B and Mokrosinska D (eds) *The social dimensions of privacy: Interdisciplinary perspective,* Cambridge University Press, 2015, 228 – 231.

74 Solove DJ, 'The meaning and value of privacy', 79.

75 Dewey J, 'Liberalism and civil liberties' in Boydston JA (ed) 2nd, *The Later works of John Dewey,* Southern Illinois University Press, 374.

76 Section 14(c), *Constitution of Kenya* (1963).

77 Rees, C, 'Tomorrow's privacy: personal information as property' *3(4) International Data Privacy Law*, 2013, 221.

78 Lessig L, 'Privacy as property' 69(1) *Social Research: An International*, 2002, 256-257.

79 Samuelson P, 'Privacy as intellectual property?' 52(5) *Stanford Law Review*, 2015, 1138 – 1139.

80 Schwartz PM, 'Property, Privacy, and Personal Data', 117(7) *Harvard Law Review,*2004, 2090 –2091.

a domino effect of exposing individuals to new privacy violations.[81] Following this train of thought, the protection in the independence constitution proves to be inadequate; not even mentioning that this right was limitable as per the vague criteria of the public interest or the interests of other individuals.[82]

Pursuant to the constitutional review suggestions,[83] the Constitution of Kenya, 2010, widens the scope of protection of the right to privacy to explicitly include a safeguard for personal information and private affairs of an individual.[84] It provides that such information should not be 'unnecessarily required or revealed'.[85] Albeit, the right is still limitable according to Article 24; however, the grounds upon which the right may be limited are significantly more stringent.[86] In line with the Constitutional Review Committee's reflections, Article 24 sets out a closed and detailed list of factors to be considered where the enjoyment of rights may be limited. Parallel to this, the independence constitution's blanket permission for limitation of rights without delineating requirements for the limitation was identified as a point for rectification of the constitution.[87]

Nonetheless, the position of the right to privacy can still be considered precarious, even under the 2010 constitutional dispensation. Despite the robust protection detailed in the Constitution, the government, which is ironically meant to be its defender, has violated it several times.[88] Not only is this exemplified by the Huduma Namba Registration process discussed above, but also by the grant of extensive monitoring and surveillance powers to state actors to 'collect and access the data [of a] mobile phone user'[89] and to access telecommunications' systems without court orders.[90] The somewhat historically precarious position that the right to privacy has long occupied sets the stage for the drafters of the DPA to grossly misconceive the right to privacy in section 28(2)(c). Contrary

81 Schwartz PM, 'Property, Privacy, and Personal Data', 2094.

82 Section 14, *Constitution of Kenya* (1963).

83 Constitution of Kenya Review Commission, *The final report of the constitution of Kenya review commission*, 2005, 122.

84 Article 31(c), *Constitution of Kenya* (2010).

85 Article 31(c), *Constitution of Kenya* (2010).

86 Article 24, *Constitution of Kenya* (2010).

87 Constitution of Kenya Review Commission, *The final report of the constitution of Kenya review commission*, 2005, 126.

88 National Coalition of Human Rights Defender-Kenya (NCHRD-K), the Kenya Legal & Ethical Issues Network on HIV and AIDS (KELIN), Paradigm Initiative, and Privacy International, *The right to privacy in Kenya*, 2019, 4.

89 Privacy International and the National Coalition of Human Rights Defenders in Kenya, *The right to privacy in Kenya,* 2015, 6

90 Privacy International and the National Coalition of Human Rights Defenders in Kenya, *The right to privacy in Kenya,* 2015, 9.

to the constitutional protection afforded, the perception of privacy adopted in section 28(2)(c) misconceives privacy by failing to understand its value where personal data is concerned. Thus, the author's argument is that this failure to grasp the inherent value of privacy culminates in the inclusion of a license permitting data controllers to indirectly collect personal information from a source which the data subject had consented previously to its collection. To establish this gross undervaluation of privacy within the Kenyan data protection scene, the Huduma Namba and NIIMS rollout provide invaluable insight and collectively set the stage for section 28(2)(c)'s misinterpretation of privacy to be demonstrated as the author will elucidate.[91]

As aforementioned, the Huduma Namba scheme was an initiative of the Kenyan government to collect and consolidate personal information from its citizens through registration facilitated by its biometric identity management system, NIIMS. The government haphazardly embarked on this voyage calling Kenyans to cede their personal information, yet there was no data protection law in existence.[92] The Kenyan government's negligence in considering privacy on this front displays its undervaluation of the right to privacy as afforded in Article 31 where it is provided that personal information should not be 'unnecessarily required'.[93] The government already held a proportion of this personal information scattered among different government agencies. For example, the National Registration Bureau which is responsible for the issuance of national identification cards, already held a register of the following personal information: name, sex, tribe or race, date of birth, place of birth, place of residence and occupation among other information.[94] Therefore, this further collection may be deemed unnecessary under Article 31.

Consequently, claims against the Huduma Namba registration were brought before the High Court in the case of *Nubian Rights Forum and 2 others v Attorney General and 6 others*. In this case, the petitioners brought a claim to the High Court challenging the implementation of the NIIMS system. They challenged its implementation on the grounds that the proposed information to be collected was excessive. Secondly, the DPA had yet to be operationalised

---

91 The Huduma Namba is referenced here to exhibit the estimation of privacy within the Kenyan data protection scene to better contextualise the argument that section 28(2)(c) is exceedingly permissive and a danger to personal data. The intention here is to showcase the legislator's understanding of privacy as they are the driving force behind the Huduma Namba roll-out and Section 28(2(c) Data Protection Act.

92 Privacy International and National Coalition of Human Rights Defenders-Kenya, *The State of Privacy in Kenya,* 2019.

93 Article 31(c), *Constitution of Kenya* (2010).

94 Section 5, *Registration of Persons Act* (Cap 107 of 2012).

leaving personal data vulnerable. Finally, that the limitation on the right to privacy was unjustifiable. Ruling in the petitioners' favour, the court found that NIIMS was unconstitutional due to the lack of an operationalised framework to protect personal data. Additionally, the High Court held that the lack of an adequate legislative framework to protect the personal information proposed to be collected, especially DNA and GPS coordinates, was an unjustifiable limitation of the right to privacy.[95] This exercise exhibits the Kenyan government's failure to satisfactorily appreciate the value of the right to privacy which eventually culminated in the formulation of the exceedingly permissive license in section 28(2)(c).

The GDPR can be considered the best practice standard as it is a development of the preceding Fair Information Practices.[96] Additionally, it has been recognised as the gold standard for data protection as it introduced the strictest protection for the right to privacy.[97] The GDPR has also received great reverence from several countries modelling their own data protection laws based after it and Kenya is one of such countries.[98] Against this background, Section 28(2)(c)'s misinterpretation of privacy by giving data controllers excessive permissions with inadequate safeguards to protect privacy can thus be established. The Kenyan government's near importation of the European GDPR law to serve as a local data protection legislative framework best illustrates this. The consequence that follows this is an oversight of the local context. Where there is a greater appreciation of the right to privacy in Europe, not only by governments but also by data controllers and processors brought on by years of practice, the same cannot be said for Kenya. Unlike Article 14 of the GDPR which places strict requirements on the data controller to notify the data subject of collection, particularly a stipulation of timelines for this notification to be made,[99] the DPA does not. A costly oversight for the data subject's right to privacy. This jeopardises privacy as the data controller may proceed to process personal data for purposes secondary to which it was initially collected for in accordance with section 30(1)(b), where consent from the data subject is not a prerequisite to processing.[100]

The importation of this permission without adequate safeguards to protect the privacy of the data subject and granting wide discretionary powers

95 *Nubian Rights Forum and 2 others v Attorney General and 6 others* (2020) eKLR, para 100.

96 Gellman R, 'Fair information practices: A basic history', SSRN Electronic Journal, 2014, 10-12.

97 Butarelli G, 'The EU GDPR as a clarion call for a new global digital gold standard', 6 *International Data Privacy Law,* 2016, 77-78.

98 Access Now, 'Data protection in Kenya: How is this right protected?', 2021, 2.

99 Article 14(3), *General Data Protection Regulation* (2016/ 679 of the European Parliament).

100 Section 30(1)(b), *Data Protection Act* (Act No. 24 of 2019).

to controllers leaves personal information extremely vulnerable at the hands of less seasoned data controllers and processors who may not fully appreciate the concept of privacy.

IV. The shortcomings of section 28(2)(c) of the Data Protection Act

Given that the DPA is fairly new, there have been few scholarly works generated on it so far. Moreover, the privacy problems of secondary use and exclusion recognised within the information processing category of the taxonomy have not been sufficiently addressed in existing Kenyan literature. This Part of the article breaks this silence by dissecting and critiquing the provisions of section 28(2)(c) and the opportunities it creates for secondary use and exclusion to prevail.

i. Accessibility and availability: Connotations of permission to use?

Section 28(1) of the DPA concerns itself with the collection of personal data setting out the general rule that all personal data should be collected from the data subjects themselves.[101] Section 28(2) sets out the circumstances in which personal information may be collected without the permission of the data subject: exceptions to the general rule.[102]

The exception presented in section 28(2)(c) contravenes the right to privacy by conflating availability and accessibility of personal data from a source that is not the data subject themselves with licence to use. Perhaps, the assumption is that the permission granted to the primary data controller to collect such information extends to the subsequent data controllers.[103] Yet, the right to privacy in Article 31(c) provides that the individual's personal data should not be unnecessarily disclosed.[104] The permission granted in section 28(2)(c) is a glaring illustration of such an unnecessary disclosure of the private affairs of an individual. Such unveiling of personal information may be considered unnecessary where an explanation for collection of information pertaining to private affairs is not

[101] Section 28 (1), *Data Protection Act* (No. 24 of 2019).

[102] Section 28(2), *Data Protection Act* (No. 24 of 2019).

[103] Lechtrek M, 'Research ethics in secondary data: what issues?' Data Big and Small, 18 May 2021-<https://databigandsmall.com/2015/10/18/research-ethics-in-secondary-data-what-issues/> on 8 March 2022. But See: Martani A, Darryl L, Pauli C, McLennan S and Simone B, 'Regulating the secondary use of data for research: Arguments against genetic exceptionalism' Frontiers in Genetics, 20 December 2019-<https://www.frontiersin.org/articles/10.3389/fgene.2019.01254/full> on 8 March 2022.

[104] Article 31(c), *Constitution of Kenya* (2010).

rendered or sought.[105] The connection between Article 31(c) and Section 25(e) which provides for the principles of data protection emerges from the object and purpose of the DPA. According to the Act, its object is to 'protect the privacy of individuals'[106] giving effect to Article 31(c) of the Constitution. Section 25(e) explicitly requires that data controllers see to it that information relating to the family and private affairs of an individual are collected only where a valid reason is provided.[107] In the same vein, Article 31(c) protects the same information from being unnecessarily revealed or required. Nexus may be drawn here such that the principle set out in Section 25(e) delineates the requirement to provide valid reasons to prevent unnecessary revelation of the information.

Where personal data is indirectly collected, the data controller would usually have not corresponded with the data subject prior to this collection.[108] This means that the data controller would have not had an opportunity to give reasons for the collection which would not be the case if consent was sought prior to collection. Additionally, Section 28(2) does not create a requirement for the data controller to disclose the reasons for this indirect collection as a prerequisite to collection.

Protection of privacy from unnecessary disclosure can be done by the purpose specification principle, which is recognised as a principle of data protection in Section 25.[109] The purpose specification principle requires that a data controller discloses to the data subject the purpose of the collection of their personal data before or at the point of collection.[110] Additionally, the DPA requires that such data may not be processed for purposes incompatible with the purposes expressed upon collection.[111] More precisely, the DPA requires that the collection be for an 'explicit, specified and legitimate purpose'.[112] The importance of the purpose specification principle cannot be downplayed as it is so central to data protection that it has been referred to as the 'cornerstone' of the GDPR.[113]

---

105 Section 25(e), *Data Protection Act* (No. 24 of 2019).

106 Section 3(c), Data Protection Act (No. 24 of 2019).

107 Section 25(e), *Data Protection Act* (No. 24 of 2019).

108 *<4D6963726F736F667420576F7264202D20B6A1B1B5A6ACB6B0ADD3A448B8EAAEC6A4A4AABAB8EAB054C576B0DDC3442D656E> (gpdp.gov.mo) on 31 May 2022.

109 Section 25(c), *Data Protection Act* (No. 24 of 2019).

110 Cannataci J and Bonnici J, 'The end of the purpose specification principle in data protection' 24(1) *International Review of Law, Computers and Technology*, 2010, 101-102.

111 Section 25(c), *Data Protection Act* (No. 24 of 2019).

112 Section 25(c), *Data Protection Act* (No. 24 of 2019).

113 Jasmontaite L, Kamara I, Zanfir-Fortuna G and Leucci S, 'Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR' 4(2) European Data Protection Law Review, 180.

This specification of the purpose works to balance the interests of data subjects and data controllers. It allows the data subject to make an informed decision on disclosure and gives them the opportunity to trace their data.[114] This requirement to disclose the purpose for data collection is inherently connected to the condition for prior informed consent as a pre-requisite for processing collected personal data.[115] Prior informed consent is the requirement that consent must be provided by a subject who is properly made aware of 'what exactly he or she is consenting to and is thus able and enabled, to some extent, to assess the consequences such consent may have'[116] before granting such consent. It allows individuals to exercise control over their personal information, hence preserving their privacy.[117] Rightly so, as consent of the data subject is the cornerstone of data protection.[118]

The further collection of personal information from a source that the data subject had previously consented to in the circumstance presented by section 28(2)(c) exposes such information to the risk of being revealed unnecessarily, effectively contravening Article 31(c). This problem may be attributed to the lack of safeguards in place to ensure that the data subject's personal information remains safe where it is held by data controllers. These safeguards may include those such as a requirement to revert to the data subject to seek consent before the information is shared again and a requirement that the information be further collected for the same purpose as it was rendered by the data subject for. Cognizant that the DPA heavily borrows its provisions from the GDPR, it should have taken note of the conditions for collection set out in article 5(1)(b) of the GDPR where the purpose specification principle is considered. Among the prerequisite conditions for collection of personal information is that the data should not be further processed for purposes incompatible with the original purpose of collection.[119] Further collection without an explicit requirement for purpose compatibility creates an opportunity for further processing that is not in alignment with the original purpose to manifest. The framing of the exception in

---

114 Cannataci J and Bonnici J, 'The end of the purpose specification principle in data protection', 102.

115 Section 30, *Data Protection Act* (No. 24 of 2019).

116 Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law, 10 SCRIPTed 4, 2013, 437.

117 Holm S and Ploug T, 'Eliciting meta consent for future secondary research use of health data using a smartphone application - a proof of concept study in the Danish population' 18(51) *BMC Medical Ethics,* 2017, 2.

118 Brownsword R, 'Consent in data protection law: Privacy, fair processing and confidentiality' in Gutwirth S, Poullet Y, Hert PD, Terwangne CD and Nouwt S (eds), *Reinventing data protection?*, Springer, 2009, 87.

119 Article 5(1)(b), *General Data Protection Regulation* (2016/ 679 of the European Parliament).

question creates room for this to occur thereby defying the purpose specification principle.

Additionally, permitting indirect collection of personal data without the condition for further consent to be sought disenfranchises the data subject from exercising control over their personal information. Hence, it leaves personal data vulnerable. As established above, a significant element of the right to privacy is the data subject's entitlement to exclusive control over access and use of their personal information. Indirect collection undercuts this element of the right to privacy as it precludes the possibility of the data subject exercising this control over their information.

ii. Secondary use and exclusion

Where the data subject is deprived of control over his personal information, room for privacy violations to manifest is created. In particular, personal data is left vulnerable to the privacy violations of secondary use and exclusion where indirect collection is permitted as is the case with section 28(2)(c).

Secondary use refers to a situation where personal information that has already been collected from the data subject is further used for a purpose different from the original purpose it was collected for. For further use to qualify as secondary use, the consent of the data subject ought not to have been sought.[120] Additionally, secondary use may also introduce the prospect of other data controllers aside from the primary collector using and processing the data.[121]

This bypassing of consent has been frowned on several occasions with scholars such as CJ Kalman, noting that, 'the requirements to seek an individual's consent to participate and to provide data for a specific purpose must take precedence'.[122] Informed consent is a prerequisite for the processing of personal information as recognised in the DPA,[123] functioning as a safeguard against abuse of personal data and in the interest of upholding the right to privacy. However, where secondary use is concerned, this consent is not obtained. This is because, at the point of collection, data controllers are unable to foresee and

[120] Solove DJ, 'A taxonomy of privacy', 490.

[121] Martani A, Geneviève LD, Pauli-Magnus C, McLennan S and Elger BS, 'Regulating the secondary use of data for research: Arguments against genetic exceptionalism'10 *Frontiers in Genetics*, 2019, 2 -< Frontiers | Regulating the Secondary Use of Data for Research: Arguments Against Genetic Exceptionalism | Genetics (frontiersin.org)> on 20 November 2021.

[122] Kalman CJ, 'Increasing the accessibility of data' 309 *The British Medical Journal,* 1994, 740.

[123] Section 30(1), *Data Protection Act* (No. 24 of 2019).

disclose the future specific uses for which the data may be used.[124] Consequently, secondary use obtains privacy violation status as it excludes the possibility of a data subject enjoying their right to privacy as it pertains to exercising control over their personal information.

On the other hand, exclusion presents a scenario where the data subject is unaware of the data that is possessed of himself and is not afforded the opportunity to participate in its handling.[125] This is extremely concerning to data subjects as they desire control over their personal data and how it is used in the interests of preserving their privacy.[126] The threat of exclusion is posed by indirect collection as there is no explicit requirement to seek further consent which would present an opportunity for the data subject to be informed. Exclusion renders personal data vulnerable as the data subject is disarmed of control over valuable information about himself.[127] This privacy violation makes way for data misuse and abuse to occur.

Reverting to the principles of data protection set out in section 25 of the DPA, there is a requirement to process data in a manner that is transparent.[128] This requirement serves to uphold the right to privacy. To do this, it necessitates that the data subject is kept up to date with their personal information. This allows the data subject to continue to exercise a level of control over their data as they may object to certain uses of their information and update as well as rectify their information when necessary.[129] However, with the permissiveness of the license given to data controllers in section 28(2)(c), the transparency requirement may not be fulfilled allowing the perpetuation of exclusion.

Section 28(2)(c) allows data controllers to collect personal data from sources which the data subject had previously consented to, threatening the safety of personal data, and creating an opportunity for the constitutionally afforded right to privacy to be violated. Furthermore, it also undermines other provisions in the DPA that seek to safeguard the right to privacy, particularly the principles of data protection as provided for in section 25 of the DPA. To exemplify, the fundamental purpose specification principle is undermined by the permission in section 28(2)(c). Thus, calls to remedy this permission are necessitated.

---

124 Law M, 'Reduce, Reuse, Recycle: Issues in the Secondary Use of Research Data' 29(1) *IASSIST Quarterly*, 2006, 6.

125 Solove DJ, 'A taxonomy of privacy', 490.

126 Meis R and Heisel M, 'Computer-Aided Identification and Validation of Intervenability Requirements' 8 *Information* 1, 2017, 1.

127 Solove DJ, 'A taxonomy of privacy', 523.

128 Section 25(b), *Data Protection Act (No. 24 of 2019)*.

129 Solove DJ, 'A taxonomy of privacy', 523.

V. Meta Consent as the solution

Following the establishment of the insecurity that personal information is exposed to, identifying a possible solution that could remedy it is the next task of this article. The proposed solution is the meta consent model. This part of the research illustrates how this concept is applicable.

i. Meta consent: The concept

Meta consent is a model of consent that allows the data subject to dictate the how and when they wish their consent to be sought for further collection and subsequent use, at the point of primary collection. It applies to personal data that has already been collected and data that is yet to be collected.[130] Simply put, it is 'a matter of designing future consent requests'.[131] Additionally, it has been described as 'consent about consent'.[132] It was first proposed within the healthcare sector as a solution to the tediousness of the informed consent model. In pursuit of advancement in the medical field, there is often need for further use of personal data collected for research purposes and, unfavourably, the informed consent model is the default model.[133] A parallel between the healthcare and data protection sectors can be drawn here as informed consent is also the default model in the data protection sector.[134]

Briefly explained, informed consent is the standard consent model that demands that the data subject with sufficient comprehension and without the influence of an outsider permits an action.[135] Thus, the conditions required for consent to be informed are that it must be voluntary, there must be understanding, and the subject must have the capacity to make decisions.[136] In the present case, the action is the collection and processing of personal data for medical research.

---

130 Holm S and Ploug T, 'Meta consent: A flexible solution to the problem of secondary use of health data', 30(9) *Bioethics,* 2016, 724.

131 Holm S and Ploug T, 'Eliciting meta consent for future secondary research use of health data using a smartphone application - a proof of concept study in the Danish population', 2.

132 Mauro S, 'Consistency in consent', Kennedy Institute of Ethics, 2019 -<Consistency in Meta Consent: A Critique – Bioethics Research Showcase (georgetown.edu)> on 3 January 2022.

133 Article 26, *World Medical Association Declaration of Helsinki: Ethical Principles for Medical Research Involving Human Subjects,* June 1964.

134 See Article 7 of the General Data Protection Regulation (2016/ 679 of the European Parliament). and Section 30(1)(a) of the Data Protection Act (No. 24 of 2019).

135 Beauchamp TL, 'Informed Consent: Its history, meaning, and present challenges', 20(4) *Cambridge Quarterly of Healthcare Ethics,* 2011, 517 – 518.

136 Hofmann B, 'Broadening consent: And diluting ethics?', 35(2) *Journal of Medical Ethics*, 2009, 125.

Acting as the cornerstone for medical research pertaining to human beings, the informed consent model is not without its own challenges.[137] The greatest obstacle presented by this model is the burden it places on healthcare researchers to seek further consent where they intend to use already collected personal data.[138] Not only is this requirement to seek further consent time-consuming, but the task of locating the data subject is often also resource intensive and in other cases impossible, for example, where the subject is dead.[139] Another unique challenge presented is the risk of 'routinisation of informed consent'.[140] This occurs where the data subject's consent is sought so often that they become desensitised resulting in 'habitual and unreflective'[141] granting of consent. This is an acute consequence of informed consent as all collection or processing of personal information requires license from the data subject. Regrettably, the impracticality of this requirement hampers research.

Informed consent proves to be challenging as it disproportionately places greater importance on the preferences of the individual while underestimating the importance of research. Hence illustrating the need for an alternative that balances the interests of researchers and data subjects in protecting their personal data. This predicament mirrors the existent problem in the data protection scene where the interests of data controllers and data subjects are juxtaposed. It may be presumed that the contentious exception in section 28(2)(c) is made to mitigate the tediousness of this informed consent model.

Meta consent comes to solve the challenges arising from informed consent. Proponents of this model in healthcare, Thomas Ploug and Soren Holm, integrate dynamic consent, broad consent, blanket consent, and blanket refusal within meta consent. These variations of consent are presented to the data subject at the first instance of collection allowing them to determine how and when they would like to provide further consent for secondary research. Practically, the data subject selects the kind of consent they desire to render for varying types of research. A prerequisite to this choice is the disclosure of the diverse types of research the data subject's personal information may be sought for by the researcher.[142]

---

137 Kadam RA, 'Informed consent process: A step further towards making it meaningful!' 8(3) *Perspectives in Clinical Research*, 2017, 107.

138 Holm S and Ploug T, 'Eliciting meta consent for future secondary research use of health data using a smartphone application - a proof of concept study in the Danish population', 2.

139 Hofmann B, 'Broadening consent: And diluting ethics?', 125.

140 Holm S and Ploug T, 'Eliciting meta consent for future secondary research use of health data using a smartphone application - a proof of concept study in the Danish population', 2.

141 Ploug T and Holm S, 'Informed consent and routinisation' 39(4) *Journal of Medical Ethics*, 2014, 214.

142 Holm S and Ploug T, 'Meta consent: a flexible and autonomous way of obtaining informed consent for secondary research', 2.

If the data subject chooses dynamic consent, their consent would be sought for every arising research that requires collection and use of their personal information. On the other hand, where a selection of broad consent is made, the subject would be approached for their consent to use their data in research of a specific kind with respect to content and context.[143] The distinction is that the former requires authorisation for every research endeavour whereas the latter only requires consultation for further consent where the research is outside the scope of the type of research consent that has already been given. Another available alternative is blanket consent where the data subject bequeaths consent for any research the researcher wishes to engage in without having to revert for further permission. This approach resembles the one taken in section 28(2)(c). Finally, blanket refusal is the circumstance in which the data subject denies any and every further collection or use of their information. Thus, their information is only used for the primary purpose for which it was collected, and they are not sought for any further permission as their preference has been expressed at the outset.[144]

Maintaining sensitivity to personal preferences, meta consent overcomes the challenges obstructing the path of informed consent. It respects the autonomy and privacy of data subjects while reducing the back and forth that accompanies informed consent leading to routinisation of consent and increased costs of research; consequently, this impedes imperative research.[145]

ii. Why meta consent?

Identical to the healthcare sector, the data protection sector has placed heavy reliance on the informed consent model. This can be seen where the DPA requires consent as a proviso to processing,[146] using,[147] and storing[148] personal data. Further, the DPA defines consent as[149]

> any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject.

---

143 Holm S and Ploug T, 'Meta consent: a flexible and autonomous way of obtaining informed consent for secondary research', 1- 2.

144 Holm S and Ploug T, 'Eliciting meta consent for future secondary research use of health data using a smartphone application - a proof of concept study in the Danish population', 2.

145 Holm S and Ploug T, 'Eliciting meta consent for future secondary research use of health data using a smartphone application - a proof of concept study in the Danish population', 2.

146 Section 30, *Data Protection Act* (Act No. 24 of 2019).

147 Section 37, *Data Protection Act* (Act No. 24 of 2019).

148 Section 39, *Data Protection Act* (Act No. 24 of 2019).

149 Section 2, *Data Protection Act* (Act No. 24 of 2019).

Thus, meta consent has been selected as the preferred solution because of its relationship with informed consent. As discussed, meta consent was proposed as a solution to cure the challenging components of the informed consent model. Its development has overcome the challenges faced by the informed consent model.

Informed consent characteristically requires several correspondences between the data controller and the data subject. This makes it a tedious process that is costly, and time-consuming[150] for data controllers and allows for routinisation of consent to fester on the data subject's part.[151] In fact, it may be assumed that the exception granted in section 28(2)(c) was made to bypass these impediments to the exploitation of personal data. However, the permission granted creates a new problem of insecurity of personal information from privacy violations. Meta consent conquers these challenges by allowing data subjects to create consent preferences from the first instance of collection.[152]

Another possible solution is data anonymisation. Data anonymisation is used where it is necessary to disclose personal information to outsiders without threatening the privacy of the data subject. Information is stripped of all personal identifiers such as names, and categories of data that may serve as personal identifiers are also modified.[153] This leaves personal data deidentified and creates an opportunity for further disclosure and use. The appeal of data anonymisation is its capacity to balance the privacy interests of the data subject and the interest in free flow of information.[154] If embraced by the Kenyan data protection regime, it would require that all personal data be deidentified prior to making it available for further collection and use.

As attractive as this model seems, it bears the risk of reidentification and deanonymisation.[155] This is the process of identifying the data subject whose personal identifiers have been removed from the information availed to third party collectors and processors. It is often done by linkage which involves the use of outside information to reidentify the data subject, among other techniques.[156]

---

150 Hofmann B, 'Broadening consent: And diluting ethics?', 125.

151 Holm S and Ploug T, 'Eliciting meta consent for future secondary research use of health data using a smartphone application - a proof of concept study in the Danish population', 2.

152 Vlahou A, Hallinan D, Apweiler R et al, 'Data sharing under the General Data Protection Regulation: Time to harmonize law and research ethics?', 77(4) *Hypertension*, 2021, 1033.

153 Ohm P, 'Broken Promises of Privacy: Responding to the surprising failure of anonymization', 57(1701) *UCLA Law Review*, 2010, 1735.

154 Ohm P, 'Broken Promises of Privacy: Responding to the surprising failure of anonymization', 1735.

155 Rubinstein IS and Hartzog W, 'Anonymization and risk', 91(2) *Washington Law Review*, 2016, 710.

156 Rubinstein IS and Hartzog W, 'Anonymization and risk', 710 - 711.

This risk continues to grow as reidentification techniques are perfected, effectively leaving personal data still insecure.[157] It also has the cumulative effect of excluding the data subject from management of their personal information leading back to the problem of exclusion. Eventually, it can be concluded that data anonymisation is not a suitable solution to the problem presented in section 28(2)(c) of the DPA.

Inasmuch as meta consent is the preferred solution, it is still plagued by problems. Sophia Mauro argues that meta consent is founded on the assumption that preferences are constant and unchanging,[158] yet this is not the case. Moreover, the structure of meta consent demands data subjects to make decisions about their future preferences even though there is no way to predict future dispositions.[159] This criticism can be overcome by the requirement that the data subject should be able to update their consent preferences made possible by meta consent's online execution.[160]

Neil Manson posits that meta consent is more expensive than broad consent as a critique. He argues this as meta consent pertains to biobanks. He proposes that funding best utilised for research is instead redirected toward administrative costs.[161] Particularly where he notes that the honouring of individual preferences destabilises the assertion that *'all things being equal'* meta consent should be preferred over informed consent as it results in 'more informed and deliberated preferences than alternative models of consent'.[162] Pressing ahead, he argues that giving research participants the ability to select their preferences presents new demands for higher administrative capabilities and the challenge of continued contact with participants.[163] The latter notes that inasmuch as the age of technology has allowed correspondence between researchers and research participants to be more efficient, the problem of human inefficiency in response times is ever-present.[164] From this perspective meta consent fails on the front of cost and time effectiveness. On this front, Holm and Ploug concede acknowledging that meta

---

157 Ohm P, 'Broken Promises of Privacy: Responding to the surprising failure of anonymization', 1731.

158 Mauro S, 'Consistency in consent', Kennedy Institute of Ethics, 2019 -<Consistency in Meta Consent: A Critique – Bioethics Research Showcase (georgetown.edu)> on 3 January 2022, 1.

159 Mauro S, 'Consistency in consent', Kennedy Institute of Ethics, 2019 -<Consistency in Meta Consent: A Critique – Bioethics Research Showcase (georgetown.edu)> on 3 January 2022, 6.

160 Holm S and Ploug T, 'Meta consent: a flexible and autonomous way of obtaining informed consent for secondary research', 2.

161 Manson NC, 'The biobank consent debate: Why 'meta-consent' is not the solution?', 45(5) *Journal of Medical Ethics*, 2019, 294.

162 Manson NC, 'The biobank consent debate: Why 'meta-consent' is not the solution?', 292.

163 Manson NC, 'The biobank consent debate: Why 'meta-consent' is not the solution?', 293.

164 Manson NC, 'The biobank consent debate: Why 'meta-consent' is not the solution?', 293.

consent may be more costly that broad consent models. However, they argue that the burden of the cost should be assessed on the grounds of whether the cost matters and not solely from the basic perspective that it costs more, as the cost could after all be marginal and innocuous to the research.[165]

Aside from the criticisms, the author remains of the opinion that meta consent emerges as the best possible solution based on the following benefits. Firstly, meta consent prioritises and honours the individual preferences of data subjects to a higher degree than other models of consent [166] which have been shown to be greatly varied.[167] This is manifest in the meta consent structure that requires data subjects to design their consent preferences pertaining to the type of data sought and the contexts in which the data is sought.[168] Another benefit that the meta consent model offers is the opportunity for consent decisions to be 'more informed and deliberated' escaping the challenge of consent routinisation.[169] The meta consent model also shines on account of its allowance to data subjects to change and update their consent preferences throughout the course of their lives.[170] In comparison to informed consent, meta consent reduces the back-and-forth discourse between the data subject and data controller by allowing decisions to be made on the meta level.[171] Moreover, it ensures that the data subject maintains control over their personal information even after they have yielded it to data controllers. This is done by permitting the subject to make decisions about 'how and when they would like to be presented with a request for consent'[172] and allowing them to continually review their preferences,[173] which is not a possibility if data anonymisation is adopted.

---

165 Holm S and Ploug T, 'The biobank consent debate: Why meta consent is still the solution!' 45(5) *Journal of Medical Ethics*, 2019, 295 - 296.

166 Holm S and Ploug T, 'Meta consent: A flexible solution to the problem of secondary use of health data', 727.

167 Holm S and Ploug T, 'Eliciting meta consent for future secondary research use of health data using a smartphone application - a proof of concept study in the Danish population', 7.

168 Holm S and Ploug T, 'Eliciting meta consent for future secondary research use of health data using a smartphone application - a proof of concept study in the Danish population', 2.

169 Holm S and Ploug T, 'Meta consent: A flexible solution to the problem of secondary use of health data', 729.

170 Sheehan M, Thompson R, Fistein J, Davies J, Dunn M, Parker M, Savulescu J and Woods K 'Authority and the future of consent in population-level biomedical research', 12(3) *Public Ethics,* 2019, 227.

171 Holm S and Ploug T, 'Meta consent: A flexible solution to the problem of secondary use of health data', 724.

172 Holm S and Ploug T, 'Meta consent: A flexible solution to the problem of secondary use of health data', 724.

173 Sheehan M, Thompson R, Fistein J, Davies J, Dunn M, Parker M, Savulescu J and Woods K 'Authority and the future of consent in population-level biomedical research', 227.

iii. Meta consent: A solution to the insecurity of personal data

Section 28(2)(c) presents a fertile environment for the privacy violations of secondary use and exclusion to thrive. It undermines the object of the DPA which is to protect the personal information of data subjects as an operationalisation of Article 31 of the Constitution. Accordingly, it is pertinent that redress to this insecurity is found.

The problematic element of section 28(2)(c) is that it disenfranchises data subjects from exercising control over their personal information. Instead, it vests excessive control over personal information collected to data controllers. Conversely, meta consent allows data subjects to regain this control. It permits better protection of personal data by ensuring that data subjects maintain this control even after it has been surrendered to data controllers. [174] This may effectively cure the problem of insecurity of personal data.

Additionally, secondary use creates room for personal information to be used for purposes incompatible or even contrary to the original purpose for which it was collected.[175] Meta consent remedies this by requiring consent for all processing; albeit in different formats the data controller is required to inform the data subject of the purpose for further collection and/or use in seeking consent. This can be exemplified where the data subject has selected dynamic consent as their preferred means of granting authorisation. The data controller is compelled to seek the consent of the data subject for every new research use and, unique to this present context, for every further collection from a source that is already consensually in possession of the personal information sought. This would effectively exclude the possibility of personal information being used for purposes incompatible with the original purpose. This is because upon making the new request, the data controller may present a new purpose to the data subject and that becomes the basis of the newly granted consent. This would act as a remedy to the insecurity of personal data.

On the part of exclusion, the data subject is precluded from participating in the management of their personal information once it has been surrendered to data controllers. The usurpation of data subject's control over personal data as facilitated by section 28(2)(c) is manifest here. Inversely, meta consent

---

[174] See generally: Holm S and Ploug T, 'Meta consent: A flexible solution to the problem of secondary use of health data', 30(9) *Bioethics,* 2016.

[175] Martani A, Geneviève LD, Pauli-Magnus C, McLennan S and Elger BS, 'Regulating the secondary use of data for research: Arguments against genetic exceptionalism', 10(1254) *Frontiers in Genetics*, 2019 -<Frontiers | Regulating the Secondary Use of Data for Research: Arguments Against Genetic Exceptionalism | Genetics (frontiersin.org)>on 20 November 2021, 2 and 7.

creates room for data subjects to be involved in the handling of their personal information. This is present in the consultation necessary between the data controller and data subject as to how and when consent will be sought at the point of primary collection.[176] The instance of selecting broad consent as the preferred consent model demonstrates this. As earlier discussed, broad consent is given for collection and use of specific content of personal information in a particular context. Where the further collection and use exceeds the scope of the prior authorisation, further consent is required thereby necessitating consultation with and involvement of the data subject.

Meta consent also cures the problem of a lack of transparency that is characteristic of exclusion. Where exclusion precludes the data subject, meta consent demands consultation with the subject to determine the type of consent preferred when handling their information. Subsequently, the data subject is not only aware of who is in possession and has access to their personal information but also how it is being used. These possibilities are rendered impossible where exclusion manifests. The adoption of meta consent has the capacity to keep the data subject up to date with the handling of their personal data in the possession of outsiders. Thus, meta consent positions itself as a viable solution to the insecurity of personal data in section 28(2)(c).

VI. Recommendations

i. Feasibility of implementation of meta consent in Kenya and Recommendations

Meta consent is set to change how data subjects disclose their consent preferences in a novel way. Precisely, the functioning of meta consent is buttressed on the existence of technology and connectivity. As Ploug and Horen envision it,[177] meta consent relies heavily on ICT for these reasons:

i. For the initial collection of meta consent and the selection of consent preferences.

ii. For researchers and data controllers to make consent requests in accordance with the consent preferences made on the meta-level as noted above.

[176] Holm S and Ploug T, 'Going Beyond the False Dichotomy of Broad or Specific Consent: A Meta-Perspective on Participant Choice in Research Using Human Tissue', 15(9) *The American Journal of Bioethics,* 2015, 46.

[177] Holm S and Ploug T, 'Meta consent: a flexible and autonomous way of obtaining informed consent for secondary research', 2.

iii. For data controllers to communicate with data subjects about the said consent requests.

The data controller needs to have easy access to the data subject so as not to impede the progression of the research. Technology aids this. However, it must be noted that aside from the use for noble research purposes, collected data may be misused for shrewd purposes.[178] They also propose that this meta consent system would work best in countries where people have a 'unique personal identification code, and where citizens are already required to have a publicly authorised electronic mailbox'.[179] The latter are synonymous with email addresses; they are used to receive correspondence from public entities. The rationale is that where there is already this level of technological infrastructure, an addition for consent requests to be generated would not be a difficult leap. It would be undemanding.

Consequently, the odds are seemingly stacked against meta consent being applicable in Kenya. Presently, there is no requirement for citizens to have electronic mailboxes that are publicly authorised. Moreover, this requirement could not be plausibly implemented as there is still considerably low internet usage by Kenyans. As of January 2021, there were only 21.75 million internet users amounting to only 40 percent of the population.[180] Some citizens have personal identification numbers in the form of National Identification cards[181] and the Huduma Namba, whose roll out has now been declared illegal for violation of the DPA.[182] Briefly, the most recent High Court decision on the Huduma Namba resulted in a declaration of unconstitutionality on the grounds that the Kenyan Government began the process without a legal protection for the personal data. This resulted in a failure to appreciate the DPA's application to collection and processing of such data with the court implying that it applies retrogressively.[183]

The future of meta consent in Kenya is not grim; it is far from that. Borrowing from the leveraging of technology and innovation in the Fintech

[178] Arežina V, Spasojević N and Peković A, 'Misuse of personal data in public opinion polls – New examples in the form of internet of things devices and applications', Archibald Reiss Days, online, 9 November 2021, 343.

[179] Holm S and Ploug T, 'Eliciting meta consent for future secondary research use of health data using a smartphone application - a proof of concept study in the Danish population', 2.

[180] DataReportal, *Digital 2021: Kenya,* 2021, 17.

[181] Section 6, *Registration of Persons Act* (Cap. 107 of 2012).

[182] 'Consortium Applauds Court Judgement Declaring Huduma Cards Illegal; Calls for Further Reforms' Kenya Human Rights Commission, 18 October 2021 -<KHRC - Consortium Applauds Court Judgement Declaring Huduma Cards Illegal; Calls for Further Reforms> on 27 December 2021.

[183] 'Consortium Applauds Court Judgement Declaring Huduma Cards Illegal; Calls for Further Reforms' Kenya Human Rights Commission, 18 October 2021 -<KHRC - Consortium Applauds Court Judgement Declaring Huduma Cards Illegal; Calls for Further Reforms> on 27 December 2021.

sector by developing mobile money, provides a way for meta consent to be embraced in Kenya. As a solution to the mass population that was unbanked in Kenya and cognizant of the fast-growing mobile penetration, Fintech harnessed this connectivity to bridge the gap between financial services and the unbanked population. Launching M-Pesa in 2007, Safaricom went against the grain where banks had a monopoly over the delivery of financial services.[184] This innovation continues to be considered a successful tool in changing the lives of the unbanked, accelerating economic growth and revolutionising the delivery of financial services.[185]

Certainly, mobile penetration, may offer a solution to overcome the lack of electronic mailboxes. Recorded at a percentage of 108.9% of the population in January 2021,[186] mobile penetration provides a loophole. Data controllers and researchers may develop a system that takes advantage of the high percentage of mobile penetration to seek and collect consent via mobile phones. This way meta consent can be modified to better fit the Kenyan context, and the exceptionally high mobile penetration in Kenya may be leveraged for better protection of personal information.

The issue of digital literacy in Kenya must be considered in the implementation of this recommendation. The government is paying attention to this issue as evidenced by the digital literacy programme that is being rolled out in schools to 'equip pupils with relevant skills needed in today's digital world'.[187] Execution of this meta consent program as the author envisions it would not be a highly technical process requiring great technological know-how. The author envisions that consent requests may be shared with users via text messages, a relatively uncomplicated means of communication that most Kenyans are familiar with. The consent requests should be accompanied by clear and understandable explanations of the implications of the consent sought.

These measures are admittedly resource intensive and often frowned upon by the technology sector[188] and met with political unwillingness exhibited

---

184 Muthiora B, 'Enabling Mobile Money Policies in Kenya Fostering a Digital Financial Revolution', GSMA, 2015, 8.

185 Chalikopoulou E, 'What Kenya can teach its neighbours — and the US — about improving the lives of the "unbanked"', Vox, 11 September 2020 -<How M-Pesa, Kenya's mobile money banking, transformed the lives of the poor - Vox> on 27 December 2021.

186 DataReportal, *Digital 2021: Kenya,* 2021, 17.

187 Ogolla K, 'Digital Literacy Programme in Kenya; Developing IT Skills in Children to align them to the Digital World and Changing Nature of Work-Briefing Note,' World Bank -<KennedyOgolaEntryDigitalLiteracyKenya.pdf (worldbank.org)> on 6 June 2022.

188 Kwok R, 'How companies can do data protection better', Kellog Insight, 4 October 2021 -< How Companies Can Do Data Privacy Better (northwestern.edu)> on 6 June 2022.

by the government's violations of the right to privacy.[189] However, the right to privacy is a recognised fundamental right that must be safeguarded pursuant to the Constitution and other human rights instruments Kenya is party to. Thus, inasmuch as there may be resistance to the proposed solution technology companies and the government are mandated to respect and protect the right to privacy from undue interferences.[190] Better protection of fundamental right of privacy is beneficial for all stakeholders as it places the country on a level playing field with other states on the international plane. This is attractive as Kenya seeks to establish herself as Africa's silicon savannah as the world rapidly digitises its functioning and Kenya also recognises data protection as an enabler for its development of the digital economy.[191]

This research recommends the use of a pilot project that attempts to implement meta consent to curb secondary use and exclusion. Pilot projects are instrumental in the research and development phase of an innovation.[192] They are preferred since amending such an important provision without a guarantee of feasibility would be disastrous. This project should be oriented toward exploring the practicality of this solution by the use of mobile phones and the value of consent granted under such conditions.

Thereafter, the onus would then fall on legislators to amend the DPA to embrace the model. Nonetheless, this research notes the grave dangers posed to the privacy of personal information, if the permission granted in this section persists. Hence, it advances that the Judiciary may play a role in remedying section 28(2)(c). It should embrace meta consent as a solution to matters brought before it, cognizant of the fact that legislating tends to be a long and drawn-out process. This action would follow the judiciary's possible finding (within its mandate to determine the constitutionality of legislative provisions)[193] that section 28(2)(c) is unconstitutional. Consequently, backed by separation of powers,[194] the judiciary

189 See Andere B, 'Kenya's sneak attack on privacy: changes to the law allow government access to phone and computer data', AccessNow, 27 January 2021-<Kenya's sneak attack on the right to privacy - Access Now>, United States Department of State, 2020 country reports on human rights practices: Kenya, 20 March 2021 and Privacy International and the National Coalition of Human Rights Defenders in Kenya, *The right to privacy in Kenya*, 2015, 2 - https://privacyinternational.org/sites/default/files/2017-12/UPR%20Kenya.pdf on 10 May 2022.

190 See Article 31(c) of the Constitution of Kenya, Article 11 of the Universal Declaration on Human Rights and Article 17 of the International Covenant on Civil and Political Rights.

191 Ministry of Information, Communications and Technology, *Digital Economy Blueprint: Powering Kenya's transformation*, 2019.

192 -<Pilot Studies: Common Uses and Misuses | NCCIH (nih.gov)>- on 6 January 2022.

193 Article 165(d), *Constitution of Kenya* (2010).

194 Waldron J, 'Separation of Powers in Thought and Practice?', 54(2) *Boston College Law Review*, 2013, 438.

would be within its limits to declare the same as a check and balance of the legislature for legalising an erroneously permissive licence to data controllers. Furthermore, the judiciary is endowed with judicial independence[195] allowing it to act impartially without coercion from outside influences.[196] It may then introduce meta consent as a solution in declaring section 28(2)(c) unconstitutional.

VII. Conclusion

This article agitates for better protection of personal information. In pursuit of this objective, the author grounds their research in Daniel Solove's taxonomy of privacy; a conceptual framework which categorises privacy violations with a view to demystifying the often-misunderstood concept of privacy. Guided by this framework, the author presents their core thesis that section 28(2)(c) proposes a substantial risk to the privacy of personal information leaving it vulnerable to privacy violations and, establishes the necessity for rectification of the same. The privacy violations that section 28(2)(c) renders personal information vulnerable to are identified as secondary use and exclusion, as recognised by the taxonomy of privacy.

Thereafter, to further illustrate the problematic effect of section 28(2)(c), a discussion on the position of privacy and the right to privacy in the Kenyan context is embarked on. Here the author finds that the misunderstanding of the concept of privacy by the Kenyan government lays the foundation for the excessively permissive and dangerous provision of section 28(2)(c) to exist. It is against this background that the solution of meta consent is introduced to remedy the insecurity of personal data at the hands of section 28(2)(c). The consideration of the meta consent model in the healthcare sector and the possibilities of adoption in the Kenyan data protection sector allows the study's overarching objective to be met, which was to investigate whether the permission granted in section 28(2)(c) leaves personal data susceptible to privacy violations of secondary use and exclusion thus threatening the right to privacy. The model provides an avenue for better protection of personal information from privacy violations of secondary use and exclusion fulfilling the constitutional right to privacy. This study hopes that legislation and judicial decisions that embrace this solution will usher Kenyan citizens into a reality where personal data is better protected.

---

[195] Article 160, *Constitution of Kenya* (2010).

[196] Were BO, 'Judicial Independence as a Contemporary Challenge: Perspectives from Kenya', 1(1) *Comparative Law Working Papers*, 2017, 365- 366.