ANALYSING THE VIABILITY OF 'LEGITIMATE INTERESTS' AS A LAWFUL MEANS OF PROCESSING PERSONAL DATA.

Submitted in partial fulfillment of the requirements of the Bachelor of Laws Degree,

Strathmore University Law School

By

[Yvonne Mbaika Mule]

[139107]

Prepared under the supervision of

Kelvin Wachira Mbatia

[February 2025]

10,035 Words

Declaration

I, Yvonne Mbaika Mule, do hereby declare that this research is my original work and that to the best of my knowledge and belief, it has not been previously, in its entirety or in part, been submitted to any other university for a degree or diploma. Other works cited referred to are accordingly acknowledged.

Signed: .....

Date: .....28.02.2025.....

This dissertation has been submitted for examination with my approval as University Supervisor.

Signed:.....

[Supervisor's Name]

Date: 28th February 2025

ACNOWLEDGMEMTS

To God, to my father Daniel Mule, my aunt Mukenyi and my sister Michelle for their never ending support, to my mother for her love which drives me every day, to my supervisor for his guidance throughout this process, thank you.

LIST OF ABBREVIATIONS:

AI- Artificial Intelligence

EAC- East African Community

ECOSOC- The Economic and Social Council

EDPB – European Data Protection Board EU- European Union

GDPR- General Data Protection Regulations

IT- Information Technology

NYOB- The European Center for Digital Rights

ODPC- Office of the Data Protection Commissioner

UN- United Nations

INDEX OF LEGAL INSTRUMENTS:

The Constitution of Kenya 2010

Data Protection Act Kenya 2019

The Data Protection General regulations 2021

The General Data Protection Regulations (EU) 2016/679

LIST OF CASES:

Meta Platforms Inc v Bundeskartellamt (2023), Court of Justice of the European Union

Patel v Facebook (2019), Appellate Court, United States, North America.

Winston Smith v Facebook (2018), United States court of Appeals

Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others (2020), eKLR.

Orange Romania SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (2020), Court of Justice of the European Union,

ANALYSING THE VIABILITY OF 'LEGITIMATE INTERESTS' AS A LAWFUL BASIS FOR PROCESSING PERSONAL DATA.

ABSTRACT

Personal data is indivisible from the person. It contains information on patterns of behavior, personal preferences and a person's overall identity. Technology continues to grow at a rapid rate and personal data therefore needs to be afforded a similar level of rights and protections that would accrue to an individual. This will ensure that there is safeguarding of people's privacy, dignity and even their autonomy.

Various strides have been made in order to give this protection, including providing for specific grounds by which personal data may be lawfully processed. Among these grounds however, is one ground whose ambiguity carries with it a large potential for misuse or abuse. This reference is made in accordance with the '' legitimate interests '' ground.

This research seeks to investigate the legitimate interest ground and to examine the rationale for its creation, its impact in data processing thus far and to make recommendations on whether it should be limited to certain actors such as the state. It also seeks to consolidate the information available about this ground in order to bring clarity on what it covers and what falls outside its scope.

CHAPTER ONE:

1.1 Introduction

The Constitution of Kenya recognizes the fundamental nature of privacy to the person. Under Article 31(c) and 31(d), the right to privacy in communication as well as protection of information to do with one's family and private affairs is granted.[1] A direct quote from Justice Mativo notes that '...the collection and distribution of personal information creates a direct threat to an individual's privacy.'[2] When people's information is arbitrarily collected, processed and stored, there is then a direct line to the violation of the individual's privacy.

Personal data is any data that can be used to identify a natural person.[3] Where a person has given consent to the collection of their personal data, one may assume that they considered and weighed the risks of mass collection versus their need to access the service being provided. However, where "'legitimate interests'" is the relied upon ground, data subjects[4] are often denied the opportunity to weigh the benefits and costs of the collection of their personal information by data controllers.[5]

The term ''legitimate interests'' is mentioned eleven times within Kenya's Data Protection Act, yet it is not defined. The Kenyan Data Protection Act is closely modelled after the European Union's General Data Protection Regulations (GDPR) and so in the absence of a definition within Kenya's Act then it would be prudent to look towards the GDPR as well as other relevant jurisprudence to decipher the meaning of "'legitimate interests'"

[1] Article 31, Constitution of Kenya (2010)

[2] Okiya Omtatah Okoiti v communications Authority of Kenya & 8 others (2020), eKLR

[3] Section 2, Data Protection Act of Kenya, 2019.

[4] Section 2 of Kenya's Data Protection Act defines this term as an identified or identifiable natural person who is the subject of personal data

[5] Kenya's Data Protection Act defines this a natural or legal person. Public authority, agency or any other body which, alone or jointly with others, determines the purpose and means of processing of personal data.

Although the GDPR itself does not define ''legitimate interests'', the GDPR recitals, specifically recital 47, note that 'legitimate interests' may be present where a data subject is a client or in service of the data controller. Moreover, one would need to make an assessment as to whether a data subject would reasonably expect that their personal data may be collected and processed within that particular time or context. Lastly, the Recital mentions that processing of data where it is necessary to prevent fraud is a legitimate interest and that the processing of data for direct marketing purposes may also be considered as a legitimate interest.[6] Though this gives much needed insight into the ground, it is still widely open to interpretation.

A further investigation into the meaning of 'legitimate interests' leads to the Article 29 Working Party, an independent data protection and privacy advisory body of the European Union, which defines it as a balancing test. It lists examples of possible 'legitimate interests' such as direct marketing and other forms of marketing and advertising, whistle-blowing schemes, IT and network security as well as unsolicited non-commercial messages including those made for political campaigns and charitable fundraising.[7] This interpretation is seen in various decided cases within the European Union and includes identification of a legitimate interest that is being pursued by the data controller, an assessment as to whether the collection of personal data is necessary for the legitimate interest being pursued and a balancing test to determine whether the legitimate interest overrides the interests and/ fundamental freedoms of the data subject.[8]

One may argue that the legitimate interest ground brings about flexibility in the laws regarding collection of personal data. It is important to note however, that over-flexibility may cause actors to expand their scope of power in ways that lead to undesired consequences. Moreover, the other grounds of collecting and/ processing personal data are broad and encompass situations where information is needed to comply with a contractual or legal obligation, to protect the vital interests

[6] GDPR recitals, Number 47 < https://gdpr-info.eu/recitals/no-47/ > - on 16 September 2024
[7] Opinion 06/2014 on the notion of 'legitimate interests' of the data controller under Article 7 of Directive 95/46/EC' Article 29, Data Protection Working Paper, https://www.dataprotection.ro/servlet/ViewDocument?id=1086 -on 14 September 2024.
[8] Cooper D, Young M, Maynard P and Griffiths T, 'Five key takeaways from recent EU developments on the GDPR's "legitimate interests" legal basis' Inside Privacy 18 October 2024 https://www.insideprivacy.com/data-privacy/five-key-takeaways-from-recent-eu-developments-on-the-gdprs-legitimate-interests-legal-basis/ on 20 October 2024

of an individual, for the public interest and even for research purposes. With such a comprehensive scope of collection allowances, what then is the purpose of the legitimate interest ground?

This study shall scrutinize the legitimate interest ground to effectively understand and critique the rationale behind its inclusion in data protection legislation. There shall also be a comparison of its practical implications since the time of its inclusion into the law in comparison with the objectives that lawmakers sought to achieve.

1.2 Background of the Study:

The European Center for Digital Rights (NYOB) is a non-governmental organization based in Vienna, Austria. Its main aim is to ensure enforcement of privacy rights and data protection laws across Europe especially when it would be too expensive or difficult for individuals to try and enforce their fundamental rights by themselves.[9] On the 6th of June this year, 2024, NYOB filed complaints to eleven European Data Protection Authorities about Meta's intention to change its privacy policy which would include the use of personal data to train its Artificial Intelligence (AI) technologies.[10] The basis of this use of data would be 'legitimate interests' and where a user would want to object, they would have to do so via an objection form which would have to be filled before the 26th of June.[11] This is problematic for various reasons. First, the GDPR states that personal data must be collected for certain, specified purposes.[12] According to Recital 50 of the GDPR, further processing of data other than for the reasons that the data was initially collected should only happen where the processing is compatible with the initial reasons for collection. Moreover, the reasonable expectations of the data subjects should be considered. [13] Data should not be stored for periods longer than necessary. It is likely that feeding people's data into AI will be an irreversible process and so this interferes with people's right to be forgotten as provided for by Article 17 of the GDPR.[14]

---

[9] https://noyb.eu/en/about-us on 8 October 2024.
[10] 'Meta Under Fire: Noyb Complains about Meta's Use of Personal Data to Train AI', 21 June 2024, <https://ai-regulation.com/noyb-complaints-meta-under-fire/ >on 8 October 2024.
[11] 'EU: NOYB files 11 complaints against Meta for use of data for AI training ', 6 June 2024 on 8 October 2024https://www.dataguidance.com/news/eu-noyb-files-11-complaints-against-meta-use-data-ai on 8 October 2024
[12] Section 5, General Data Proetction Regulations, 2018.
[13] GDPR recitals, number 50 - https://gdpr-info.eu/recitals/no-50/ on 8 October 2024.
[14] GDPR, article 17 - https://gdpr-info.eu/art-17-gdpr/ on 8 October 2024.

Meta has had a long history of collecting large amounts of personal data which users may not reasonably expect to be collected or to be used in such a manner and using it to develop new technologies or to create more targeted advertisements. Examples of this would be the *Patel v Facebook* case and the *Smith v Facebook* case.

In *Patel v Facebook*, it was discovered that Facebook had introduced facial recognition software which allowed users to tag the people in their pictures automatically rather than manually looking up their usernames.[15] In essence, Facebook was collecting and storing its users biometric data without any prior consent and such data was being kept indefinitely without any timeframe for its erasure or deletion from its servers and without letting its users know what protections had been put in place to ensure that this data would not be compromised. Facebook claimed that there was no proof of injury but held that biometric data is sensitive personal data which cannot be altered if its integrity were to be compromised. The collection of such data was therefore seen as a violation of privacy.

In *Smith v Facebook*, it was found out that Facebook was tracking its users whenever they visited certain healthcare related websites and that they would collect the users' personal data, including their IP addresses and sell such data to advertisers or use the information for targeted marketing within their own platform.[16] On the face of it, targeted advertising may seem to be a logical and perhaps even desirable way of receiving advertising. However, the Plaintiffs in this case felt aggrieved and rightly so because although Facebook claimed it had their consent to track them, the ordinary user would not expect that their activities on non-Facebook related websites would be tracked, and such information stored and used by Facebook for advertising and any other purposes.

In America, what is now known as the Cambridge Analytica scandal showed just how serious the risk of arbitrary collection of data by large companies such as meta could be. In this scandal, private data of more than fifty million Facebook users were harvested and used to support Donald

[15] Patel v Facebook (2019), United States Appellate Court.
[16] Smith v Facebook (2017), United States District Court, California.

Trump's 2016 presidential election campaign.[17] Generally, Cambridge Analytica would use the information they obtained to influence political outcomes by helping rebrand political parties and engineering political campaigns. Closer to home; Cambridge Analytica was said to have influenced Kenya's 2017 elections by using fake news and misinformation against the winner's political rival on issues that matter the most to Kenyans including health, infrastructure and terrorism.[18] Ultimately, one must admit that with enough information about a person, it is easy to influence their opinions on certain things. At a large scale, this has enormous consequences. In this day and age, we cannot afford to have ambiguities such as the legitimate interest ground giving such companies a loophole in data collection and processing.

1.3 Statement of the Problem

It has been established that privacy is fundamental to the human being and should therefore be afforded great protection. As illustrated by the *Smith v Facebook case*, the ordinary citizen who uses social media applications does so without the expectation of constantly having their data being collected especially when they use third party websites. Ideally, where commercial purposes are the main driving force behind the collection and processing of data, the data controller should acquire the express consent of the data subjects. This express consent should be acquired after having explicitly specified what data is being collected, how it is being collected, the purpose for such collection and the period of time for which this data will be stored and processed.

The reality today is that many large commercial companies such as Meta have access to inconceivable amounts of personal data which they have been collecting for years. There are currently about two billion users of Instagram alone, many of whom are children.[19] The type of data collected includes sensitive personal data[20] that goes to the core of a person's identity and

[17] Auchard E, 'Cambridge Analytica stage-managed Kenyan president's campaigns: UK TV' , Reuters, 20 March 2018 https://www.reuters.com/article/us-facebook-cambridge-analytica-kenya-idUSKBN1GV300/ on 9 October 2024.
[18] 'Cambridge Analytica says it worked for Uhuru Kenyatta' Nation, 3 July 2020, https://nation.africa/kenya/news/politics/cambridge-analytica-says-it-worked-for-uhuru-kenyatta-23878 on 9 October 2024.
[19] https://www.statista.com/topics/1882/instagram/#topicOverview> on 8 October 2024.
[20] According to section 2 of Kenya's Data Protection Act, sensitive personal data is data that reveals information pertaining to one's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property

which, if compromised, cannot be changed. For these companies, such information is a means of increasing their profits. For the people in question, the information speaks to the very integrity of their being.

Where malicious actors are able to obtain data about individuals through hacking or even bribery it would allow them to learn individuals' locations, patterns of behavior and other information that may lead to the realization of risks such as behavioral targeting, profiling, terrorism or cyber bullying based on people's beliefs or identities. This becomes an even bigger problem where the individuals in question were not even aware that their data was being collected and stored.

This research seeks to examine the Legitimate interest ground and make determinations on whether it is a viable ground for data processing on its own or whether it should be used in tandem with the other six data processing grounds which are; acquiring consent, processing in relation to performance of a contract, processing in compliance with a legal obligation imposed on the data controller, processing in order to protect the vital interest of the data subject or processing in performance of a task carried out in the public interest.

1.4 Research objectives.

a. To examine the interpretations and usage of the legitimate interest ground.
b. To distinguish the legitimate interest ground from other grounds.
c. To analyze and propose potential modifications of the legitimate interest ground.
d. To propose recommendations on safeguards that can be put in place to mitigate the risks that come with the use of the legitimate interest ground.

1.5 Research Questions

This research seeks to answer the following questions.

1. Whether the current interpretation and usage of 'legitimate interests' violates the privacy of citizens.

details, marital status, family details including the names of a person's children, parents, spouse(s), sex or sexual orientation.

2. Are there fundamental distinctions between the legitimate interest ground and the. other six grounds of processing personal data?
3. Whether there should be modifications put in place to alter the current understanding of 'legitimate interests'.
4. What safeguards can be put in place to mitigate the risks that may come about in the use of 'legitimate interests'?

1.6Hypothesis

The legitimate interest ground may be better applicable as a secondary step in ensuring that data is being processed legally and ethically while relying on the six alternative data processing grounds. Moreover, there should be effectuation of consent as the only ground through which corporations and other commercial parties process personal data for the protection of privacy rights and for more ethical data processing by social media companies as well as other bodies.

1.7 Significance of the Study

With the rapid growth of technology and online dependence, this research is made in pursuit of eliminating the legal and ethical ambiguity that is found in the legitimate interest ground of processing personal data. It aims at ensuring that people of all ages are able to access internet-based services, especially those from social media companies, without their personal information being compromised. It hopes to provide a mechanism for accountability from the actors who have the ability to access and collect large amounts of personal data from a wide pool of individuals.

This will be done by providing clarity on the legitimate interest ground and ensuring that there are particular parameters which govern its use rather than having it being arbitrarily applicable.

The research will be an invaluable means of furthering the discourse on data privacy and security. Finally, it will give a different perspective and insights to lawmakers on what amendments should be made to the current Data Protection Act of Kenya so that the provisions for lawful data processing grounds reflect the constitutionally recognized right to privacy with regards to communications and private information.

1.8 Theoretical Framework

The main theoretical backing of this proposal falls within the contractarianism theory which is a subset of the social contract theory. It posits that people enter into contracts with one another for their mutual benefit and they have contracts between them that define the terms of their agreements. These contracts include the duties and obligations of each party towards the other which thereby govern the interaction between them.

Thomas Hobbes is a notable proponent of this theory, and he sees it as one where rational agents enter into agreements through their own free will for the mutual benefit of both agents. Immanuel Kant's take on this theory is that morality in itself is a matter of principles that depend on the agents' viewpoints and so a 'morally wrong' act is solely based on principles that are not acceptable to all rational agents.[21]

In the context of this research one of the agents in question would be the ordinary citizens who form the bulk of the users of online applications such as Instagram and TikTok. The second agent would be the owners of these applications. The 'formal' terms of contract between these two can usually be found within the terms and conditions presented by these applications. Unfortunately, they are often verbose and filled with legal and technical jargon which users tend to skip over. This is where the contractarianism theory comes in. According to this theory, the contract therein is not just the written contract but the hypothetical one which demands that the mutual benefit of both parties be considered and that actions must be acceptable by all rational actors.

Using a social media application as a case study, agent A (the user), would want a way to connect with family and loved ones as well as to have quick access to entertainment. Some users are business owners and would also like to be connected to an audience that is interested in their products, these people are agent B. Agent C (the application owner) would like to keep high engagement levels with their application. In this scenario, agent C could create and present a quick and easy checklist that users can check in order to get a broad and basic understanding of what

[21] Springer, D 'Contractarianism' Encyclopedia of Global Justice, 2011, < https://link.springer.com/referenceworkentry/10.1007/978-1-4020-9160-5_238#:~:text=%E2%80%9CContractarianism%E2%80%9D%20refers%20to%20a%20type,principally%20those%20governing%20their%20interaction > on 1 March 2024.

agent A is interested in and what they would like to see in terms of advertisements on agent C's platform. In this way, every agent's needs and wants are taken into consideration and there is consent which works to the mutual benefit of all agents. However, the problem today is that Agent C only takes its own benefit into account. It therefore bypasses the need for consent and simply begins to collect agent A's personal data without their knowledge so as to determine what they would like to see and keep showing them such items. It collects such data citing ''legitimate interests'' in doing so. Moreover, in its terms and conditions, it is likely to have put in an unconscionable clause which states that by using the application then agent A has consented to the collection of their data.

How is this to the detriment to agent A? First, the collection of unspecified information without their knowledge or free, prior and explicit consent is a clear violation of several pre-existing laws. In the Kenyan context this would include the right to privacy with regards to their communication and private affairs.[22] Moreover, consent, as defined by the European Union's General Data Protection Regulation (GDPR) and the Kenyan Data Protection Act, is the manifestation of '*express, unequivocal, free, specific and informed indication of the data subject's wishes.*'[23] Therefore, the provisions hidden in the long winded terms and conditions that claim consent has been provided through the use of the applications and services are invalid. Additionally, some companies in Agent C's position with a large amount of data may sell such data to third parties which further infringes on the rights of Agent A.

Moreover, Agent C's use of Agent A's personal data may be infringing on their autonomy as Agent A is often bombarded with advertisements for items that they may not necessarily need, and they may end up purchasing these items. Richard Lippke, while quoting John Galbraith, states that advertising often creates desires rather than responding to them. He goes on to discuss in his own paper how persuasive mass advertising is likely to affect the development of knowledge and abilities constitutive of dispositional autonomy.[24] Such advertising tactics are the bulk of these online applications, and the collection of personal data makes such advertisements much more

[22] Article 31, Constitution of Kenya (2010)
[23] Section 2, Data Protection Act (No.24 of 2019)
[24] Lippke R, ' Advertising and the social conditions of autonomy' 8(4), Business and Professional ethics Journal, 1989, 36

targeted to the individuals and their general interests thereby having a greater effect on their autonomy.

In order for the contractualism theory to work effectively then Agent C must be seen to value Agent A's autonomy and privacy. The best manifestation of this would be by collecting explicit consent for well-defined actions that will be taken by Agent C.

1.9 Literature Review

Numerous forums have taken up the discussion of personal data and its processing but more often than not, the explanations to do with 'legitimate interests' have been vague.

In one of the Working papers by Brussel's Privacy Hub, it is noted that the 'legitimate interest' ground has been criticized as one that creates a loophole in the protection of personal data although the authors of the paper disagreed with this position. The critique of this ground in this sense comes about because of its flexibility in that, almost any reason can be characterized as a legitimate interest.[25] This proposal agrees with the critique because even when explanations for legitimate interest are given, they do not present any clear guidelines for its use.

There exists in most literature, a three-part test for determining whether a company can rely on the 'legitimate interests' as a ground for processing personal data. First, the data controller should have a legitimate interest for processing the data, there must be a need to process personal data for the legitimate interest pursued and finally there is to be a balancing act to ensure that the fundamental rights of the data subject do not take precedence over the legitimate interest of the data controller.[26]

This criteria is problematic for various reasons. The first criteria seems to be a restatement of the overall question; to determine whether you can rely on 'legitimate interests', the first step is to determine whether you have a legitimate interest and this only serves to enhance the vagueness of the ground. Moreover, it is highly subject to bias and the balancing act cannot be proven to have been done unless a case is brought to court. Overall, it leaves a lot of discretion to the data

[25] Kamara I and De Hart P, 'Understanding The Balancing Act Behind The Legitimate Interest Of The Controller Ground: A Pragmatic Approach' Brussel's Privacy Hub, working paper volume 2, 2018 on 2 March 2024.
[26] Kellenher D, 'What does legitimate interest mean? The CJEU gives its answer in Rigas", The Privacy advisor, 2017

controller who ultimately will do what benefits them the most. This further accentuates the need for this research so that a clear criterion may be brought about.

Hunton Andrews Kurth in his discussion on 'legitimate interests' gives scenarios where the legitimate interest basis may be best. He lists several cases such as in the context of employment where consent would not be seen as freely given and more relevant to this proposal, he claims that in cases where targeted advertising and content personalization is on offer then 'legitimate interests' should be relied on instead of consent.[27] This proposal disagrees with this position as even if, as claimed by the author, these instances are part of the daily data processing activities, this does not negate the need for consent. Moreover, consent is not necessarily to be asked for daily, but it is necessary to collect renewed consent where the object of processing the data changes or where new types of collection. The Office of the Data Commissioner (ODPC) in one of its guidance notes on consent also states that even consent is not a silver bullet as data processors need to ensure that data processing activities are still in line with the rights of the data subjects.[28]

Pirate parties International headquarters, a UN Economic and Social Cousel (ECOSOC) consultative member, note that violations of human rights are taking place in the digital environment daily with search engines such as google and companies like Facebook collecting large amounts of data, even sensitive personal data with or without consent and sharing information with third parties and has led to increased; business and personal life surveillance, the risk of censorship and profiling of marginalized groups.[29] It is with such potential violations in mind that this research seeks to properly define the legitimate interest ground, specify the terms of its use and advocate for consent to be properly collected.

[27] Kurth H, ' How the "legitimate interest" ground for processing enables responsible data use and innovation' Center for Information Policy Leadership, July 2021 < https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_how_the_legitimate_interests_ground_for_processing_enables_responsible_data_use_and_innovation__1_july_2021_.pdf > on 1 March 2024.

[28] Office of the Data Commissioner 'guidance note on consent' < https://www.odpc.go.ke/download/guidance-note-on-consent/?wpdmdl=9641&refresh=651539381d24b1695889720 > 9. On 29 February 2014

[29] Dr Keith Golstein et al. (on behalf of Pirate Parties International Headquarters) 'The right to privacy in the digital age' < https://www.researchgate.net/publication/328789396_The_Right_to_Privacy_in_the_Digital_Age >on 2 March 2024.

1.10 Research Methodology

This research shall be a doctrinal legal research with several primary and secondary sources of law being the point of reference. There shall be a great focus placed on the European Union's General Data Protection regulation which highly influenced Kenya's own Data Protection Act of 2019 as well as case law, text and reference books and journal articles.

1.11 Research Limitations

This research encountered various challenges which primarily can be broken down into time constraints and inadequate accessible doctrinal research resources. The limited time duration before the proposal was to be submitted limited the depth of analysis and research that could be done with regards to this topic. Moreover, some of the real-life examples presented were subject to the researcher's personal experience and so may be subject to bias.

Despite the limitations above, the research was reliant on credible sources and sought to provide candid and reliable information under this topic.

1.12 Chapter Breakdown

Chapter one comprises the introduction and background of the study. It includes the theoretical background and literature review as well as the research questions and objectives.

Chapter two examines the legitimate interest ground from its implementation to its current usage.

Chapter three evaluates the alternatives to the legitimate interest ground and assesses the modifications that could be introduced to the ground based on comparative study

Chapter four considers the information provided in the previous chapters and gives recommendations on the way forward based om these findings.

2.0 CHAPTER TWO: THE LEGITIMATE INTERETS GROUND IN DATA PROTECTION

2.1 Introduction

Privacy has been a long established and recognized right. Some have argued that it was a common law right even before it became enshrined in law.[30] This common law right protects the inviolable personality of the individual and allows them to decide whether, and to what extent, their thoughts will be communicated to others.[31] The world today recognizes the primacy of privacy rights which are enshrined in constitutions and data privacy legislations. Klaus Schwab, the founder and chairman of the World Economic Forum, describes this point in time as the fourth industrial revolution where interconnected technologies rule and manage our lives.[32] In such an era, companies that want to get ahead would agree that data is one of the most important assets that they could have. With the amount of data that companies may gain access to, it is imperative that limits be imposed and enforced. This chapter addresses the different conceptualizations of ‘'legitimate interests'' as well as the role it has played in allowing for the vast collection of data.

2.2 Historical development leading to the inclusion of ‘'legitimate interests'' as a data processing ground.

In an effort to further conceptualize the right to privacy as envisioned by international instruments such as the UN Declaration of Human Rights in 1948 and The EU Convention on Human Rights in 1950, legislators across the globe enacted data privacy legislations. Germany passed the very first Data protection legislation in 1970.[33] Soon after, the European Union introduced the EU Data Protection Directive in 1995 and under Article 8, the concept of 'legitimate interests' as a data processing ground came into existence.[34] In 2018, the General Data Protection Regulations came into force and this ground was retained.

The development of Data Protection in Africa has been much slower and this may be due to the overall conception of privacy. Some scholars like Alex Makulilo have argued that privacy is a western ideal. This view seems to be supported by some commentators such as Serge Gutwirth

[30] Glancy D, ‘THE INVENTION OF THE RIGHT TO PRIVACY’, 21, Arizona Law Review, 1, 1979, 2.
[31] Glancy D, ‘THE INVENTION OF THE RIGHT TO PRIVACY’ 2.
[32] Xu M, David J and Kim S, ‘The Fourth Industrial Revolution: Opportunities and Challenges’ 9, International Journal of Financial Research’ , 2, 2018, 90.
[33] Fuster G, ’History of data protection:1970’ Wordpress https://glgonzalezfuster.blog/history-of-data-protection-an-online-anthology/history-of-data-protection-1970/ on 7 December 2024
[34] Article 8 2(e), European Union Data Protection Directive (Directive 95/46/EC)

who argues that African values are often centered on community and that individualism is subject to the group. He further points out that the 1981 African Charter on Human and People's Rights did not even mention privacy.[35] These points of view perhaps partly demonstrate why data protection in Africa has lagged behind in comparison with developed countries. However, data regulation efforts have gained a lot of momentum. The African Union Data Policy Framework adopted in 2022, notes that there is need for a change in data regulation so that countries can benefit from the emerging global data economy.[36]

In line with the standard set by the EU, which had grappled with data protection law for a longer amount of time, Kenya adopted the same grounds for processing personal data as set out by the GDPR. These included the legitimate interest ground. Kenya's Data Protection Act specifically states that 'legitimate interests' are a lawful data processing ground "*except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or 'legitimate interests' of the data subject*"[37] This standard leaves several gaps in clarity. What level or type of processing meets the threshold of being warranted or unwarranted? What 'legitimate interests' of the data subject, beyond their constitutional rights and freedoms, are being protected?

Within Kenya's Data Protection (General) Regulations of 2021, it is also noted that 'legitimate interests' need to be connected to the specific purpose of processing.[38] Additionally, under the right to object to processing, the Act notes that 'legitimate interests' of the data processor may override this of the data subject. When such a situation occurs, the data controller shall inform the data subject of the reasons for declining the request for objection and of their right to lodge a complaint to the data commissioner.[39]

Most, if not all, legislations recognize consent as being a lawful basis for processing personal data. While some jurisdictions consider it to be one of the primary reasons to process data, some jurisdictions with Kenya included, simply see it as one of the alternatives for processing data without stipulating a hierarchy of any sort.[40] Contrastingly, the ECOWAS supplementary Act on Personal Data Protection within ECOWAS states that legitimacy in the processing of personal data is grounded upon consent.[41] Consent can only be waived where the data controller needs to comply with a legal obligation, a public interest need or exercise of public authority, performance of a contract and where there is a need to safeguard the rights and fundamental liberties of the data subject.[42]

---

[35] Gutwirth S, Privacy and the Information age' 2002, page 24
[36] Section 3, The African Union Data Policy Framework, 2022.
[37] Section 30, Data Protection Act 2019.
[38] Section 29, Kenya Data Protection (General) Regulation 2021.
[39] Section 8 (6) ,Kenya Data Protection (General) Regulations 2021.
[40] Section 44 , Data Protection Act 2019.
[41] Article 23, Supplementary act on Personal Data Protection within ECOWAS, 2010
[42] Article 23, Supplementary act on Personal Data Protection within ECOWAS, 2010

The African Union Data Policy Framework does not outline specific grounds for processing personal data. It requires its member states to come up with such legislation but it outlines several principles that processing should align with and the list begins with the principle of 'consent and legitimacy.[43] The policy framework describes the 'legitimate interests' of the state as 'the fight against money laundering, tax evasion, online gambling and national security'.[44] There is however no description of what legitimacy may be for independent individuals or organizations. It is therefore left to member states to decide what 'legitimate interests' means.

Unfortunately, even within country specific legislation, the concept of 'legitimate interest' is not defined within data protection legislation–. This inadvertently has elevated the reliance on the 'legitimate interests' ground by most potential data controllers since the laws and standards of acquiring consent are more stringent while the legitimate interest ground is largely left to the discretion of the data controller.

In Kenya, there is little clarity as to how to determine whether a data controller's interests are legitimate. The guidance note for the communication sector by the office of the data protection commissioner does however state that the legitimate interest relied upon by the controller should not outweigh the rights and freedoms of subscribers. It also states that service providers should be guided by principles such as purpose limitation, lawfulness, fairness and transparency.[45] The guidance note also issues one concrete measure of transparency. It requires that easily understandable privacy notices be given to subscribers which include the purpose of processing, the legal basis for it as well as the amount of time that the data will be held.[46] Guidelines for other industries are yet to be set out.

Although Kenya's data processing regulations are largely modelled after the EUs' framework, it lacks proper regulatory guidelines and jurisprudence that can offer guidance. Even within the EU there are several gaps, however, the usage of the legitimate interest ground is more settled in practice. In the EU, the 'legitimate interests' ground generally applies when the processing of the data is not required by law, but has a clear benefit; when such processing carries little risk of intruding into the data subject's privacy; and when the data subject should reasonably expect their data to be used for those purposes in those circumstances.[47] The GDPR includes instances of a need to prevent fraud, processing data of clients and ensuring that the networks are secure.[48] Nevertheless, a lot of discretion has generally been afforded to data controllers.

---

[43] Section VII, The African Union Data Policy Framework, 2022.
[44] Section 2.1, The African Union Data Policy Framework, 2022.
[45] Office of the Data Protection Commissioner, Guidance note for the communication sector.
[46] Office of the Data Protection Commissioner, Guidance note for the communication sector
[47] Irwin L, 'What is Legitimate Interest under the GDPR' 15th July 2024 Luke Irwin 15th July 2024https://www.itgovernance.eu/blog/en/the-gdpr-legitimate-interest-what-is-it-and-when-does-it-apply on 12 January 2024.
[48] Recital 47, General Data Protection Regulations Recitals, 2016.

2.3 Understanding 'legitimate interests'.

A working paper by Brussel's Privacy Hub makes the claim that 'legitimate interests' is not a self-standing provision but instead should be read through the lens of other data protection principles such as the fairness of processing. It also states that the positive obligations on the data controllers in terms of complying with regulation and demonstrating that they have complied with it improves accountability.[49] While this would be true in theory, I would posit that the opposite is true in practice.

The overarching problem with 'legitimate interests' remains that, there is a clear conflict of interest when it is left up to the data controllers to decide whether their interests are legitimate enough to override the rights and fundamental freedoms of the data subjects. Moreover, it may be difficult for the average citizen to realize that their personal data is being unjustly collected, utilized or sold. They would likely have a hard time understanding the extent of the data processing and the technology that is being utilized for the same not to mention the burden of demonstrating that damage in a court of law and acquiring redress.[50]

A study on the practical use of 'legitimate interests' as a data processing ground showed that its use often lacks transparency and the right to object to processing is often buried deeply within the privacy settings to prevent user interaction. [51] Only about 4% of websites of the 10,000 websites studied disclosed that the basis of their processing of data is 'legitimate interests' and even then, only 1.3% of users actually interacted with the privacy notices where this information was disclosed.[52] Since the 'legitimate interests' themselves were not actually meaningfully explained or listed to users, the question remains how exactly users can be expected to object when they do not know what it is they are objecting to or even how they are supposed to go about these objections. I believe that the onus of ensuring that users have this information is on the data controllers themselves, as they already have the power to balance their interests and user interests and rights, to determine whether they can process data under this ground.

---

[49] Kamara I and Hert P, 'UNDERSTANDING THE BALANCING ACT BEHIND THE LEGITIMATE INTEREST OF
THE CONTROLLER GROUND: A PRAGMATIC APPROACH' Brussel's Privacy Hub, 2018,15, https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf on 07 December 2024

[50] Ferretti F, 'DATA PROTECTION AND THE LEGITIMATE INTEREST OF DATA CONTROLLERS: MUCH ADO ABOUT NOTHING OR THE WINTER OF RIGHTS?' Common Market Law review, 2014, 19, https://www.academia.edu/56236925/Data_protection_and_the_legitimate_interest_of_data_controllers_Much_ado_about_nothing_or_the_winter_of_rights on 7 December 2024.

[51] Investigating Deceptive Design in GDPR's Legitimate Interest https://homes.cs.washington.edu/~franzi/pdf/kyi-legitimateinterest-chi23.pdf on 9 December 2024.

[52] Investigating Deceptive Design in GDPR's Legitimate Interest, https://homes.cs.washington.edu/~franzi/pdf/kyi-legitimateinterest-chi23.pdf on 9 December 2024.

The second limb of the 'legitimate interest' balancing test includes a determination that the processing is necessary and that the purpose for processing cannot be met by less intrusive means.[53] The large number of data controllers that rely on 'legitimate interests' for purposes such as personalized content delivery or personalized advertisements seems to be at odds with this step. The findings within the study showed that although personalized content and personalized advertisements were viewed as being distinct by users, neither one was deemed as necessary or desirable despite their wide usage as the 'legitimate interests' in data processing.[54] In fact, online behavioral advertising and consequently, profiling of data subjects is not strictly necessary in the eyes of a website user.[55] This purpose should thereby be anchored on free, informed and explicit consent of users and not on 'legitimate interests'.

Another study conducted by 'Bits of Freedom' in Amsterdam focused on 'legitimate interests' as used by Google, Facebook and LinkedIn. The sheer amount of data collected by Google is astonishing once it is fully listed out; device information, web browsing history, your phone number and the time, date, duration and types of calls or messages received and sent, your address, the date and time of all your queries and your location at all times as well as cookies that may identify your browser and much more.[56] Google has access to all and every type of data set including sensitive personal data. Google not only collects this data from its own services but also from third parties that use its advertising services. Google's stated purposes at the time of the study were to maintain and improve provided services and to improve user experience as well as the quality of its services.[57] With the volume of data collected, these reasons seem vague and insufficient. It is also hard to determine how the balancing test was conducted as against other rights such as the right to privacy, the right to object to processing of data and the right to be forgotten.

Facebook was also studied and it was shown that they also collect huge amounts of data some of which include; chat and comment history, credit card information, political and religious views, facial recognition, former relationships (people who you unfriended and who have unfriended you), the devices one uses to log into Facebook with as well other people who have logged in on that same device and the profiles that the user is most interested in.[58] Even when a user deletes their account, such records are still retained. A researcher who requested his data from Facebook

---

[53] Kamara I and Hert P, 'UNDERSTANDING THE BALANCING ACT BEHIND THE LEGITIMATE INTEREST OF
THE CONTROLLER GROUND: A PRAGMATIC APPROACH' 14.
[54] 'A LOOPHOLE IN DATA PROCESSING', Bits of Freedom, 11 December 2012.
https://www.bitsoffreedom.nl/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf
[55] A LOOPHOLE IN DATA PROCESSING', Bits of Freedom, 11 December 2012.
https://www.bitsoffreedom.nl/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf
[56] A LOOPHOLE IN DATA PROCESSING', Bits of Freedom, 11 December 2012.
https://www.bitsoffreedom.nl/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf
[57] A LOOPHOLE IN DATA PROCESSING', Bits of Freedom, 11 December 2012.
https://www.bitsoffreedom.nl/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf
[58]' Facebook's Data Pool http://www.europe-v-facebook.org/EN/Data_Pool/data_pool.html on 15 January 2024.

noted that printing the information which Facebook collects could lead to 1,200 pages per user.[59] This was the position in 2012, one can only begin to imagine how much information is being stored per user in 2024, 12 years later. Its stated 'legitimate interests' were similar to Google's and included advertising interests.

LinkedIn was also noted to have harvested a huge amount of information including confidential notes and passwords. This practice only stopped after the issue was raised by investigative individuals and a public outroar followed.[60] The study notes that most data controllers relying on 'legitimate interests' to collect personal data do not get caught and the processing continues without reasonable interests that are outside the realm of using and selling data for profit. [61]

2.4 Conclusion:

While many Academics would like to believe that 'legitimate interests' is not a loophole for unfair data processing practices, this is simply not the case in practice. In line with Adam Smiths' assertion that 'it is not from be the benevolence of the butcher or the baker that we expect our dinner, but from their regard to their own self-interest', companies that offer services, especially 'free services' do not do so simply because they are benevolent. 'If you are not paying for the product then you are the product'[62] and unfortunately, due to the laws in place, people's information, their data and the consequential influence on their opinions and actions has become a legal product.

[59] A LOOPHOLE IN DATA PROCESSING', Bits of Freedom, 11 December 2012. https://www.bitsoffreedom.nl/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf
[60] A LOOPHOLE IN DATA PROCESSING', Bits of Freedom, 11 December 2012. https://www.bitsoffreedom.nl/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf
[61] A LOOPHOLE IN DATA PROCESSING', Bits of Freedom, 11 December 2012. https://www.bitsoffreedom.nl/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf
[62] Goodson S, 'If you're not paying for it, you become the product ' Forbes, 14 April 2022 https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/ on 8 December 2024.

3.0 CHAPTER THREE: ALTERNATIVES AND MODIFICATIONS TO THE LEGITIMATE INTEREST GROUND.

3.1 Introduction

The overarching question here is whether 'interests' of people or businesses should prevail over pre-existing rights such as the right to privacy. This is especially where the interests themselves are not predetermined or outlined. A staunch criticism of the 'legitimate interests' balancing test notes that where interests are balanced over fundamental rights rather than balancing rights against other rights, this lowers the protection that is due to the pre-existing and defined rights.[63]

Currently, there are several initiatives being undertaken in East Africa with the purpose of consolidating ideas and coming up with joint frameworks for data governance. These initiatives hope to culminate in the creation of a digitally interconnected region that will foster innovation, facilitate easier cross border data flow and encourage investment in the region's digital economy.[64] Some of these projects are joint ventures with the EU such as the Data Governance in Africa Initiative and the African Union European Union (AU-EU) Digital for Development (D4D) Hub Project).[65] Notably, the first adequacy dialogue between the EU and a country on the African continent began in 2024 with Kenya.[66] Adequacy talks may lead to an adequacy decision which is a finding that the jurisdiction in question has a similar level of data protection to the EU thus data can flow freely between the two jurisdictions.[67] The goal of these talks is to increase the benefits from the recently concluded EU-Kenya partnership agreement by improving cross-border trade in

---

[63] Guinchard A, *'Taking proportionality seriously: The use of contextual integrity for a more informed and transparent analysis in EU data protection law'* , European Law Journal, 2018, 10.

[64] 'EAC readies to accelerate regional digital integration with cross-border data flow framework', 24 December 2024 — < https://www.eac.int/press-releases/3287-eac-readies-to-accelerate-regional-digital-integration-with-cross-border-data-flow-framework >on 2 January 2025

[65] Opening remarks by European Union Deputy Ambassador Ondrej Šimek at the Network for African Data Protection Authorities (NADPA) Conference , 7 May 2024 <https://www.eeas.europa.eu/delegations/kenya/opening-remarks-european-union-deputy-ambassador-ondrej-%C5%A1imek-network-african-data-protection_en?s=352 > on 13 January 2024.

[66] Opening remarks by European Union Deputy Ambassador Ondrej Šimek at the Network for African Data Protection Authorities (NADPA) Conference , 7 May 2024< https://www.eeas.europa.eu/delegations/kenya/opening-remarks-european-union-deputy-ambassador-ondrej-%C5%A1imek-network-african-data-protection_en?s=352 >on 13 January 2024.

[67] Opening remarks by European Union Deputy Ambassador Ondrej Šimek at the Network for African Data Protection Authorities (NADPA) Conference , 7 May 2024 <https://www.eeas.europa.eu/delegations/kenya/opening-remarks-european-union-deputy-ambassador-ondrej-%C5%A1imek-network-african-data-protection_en?s=352 >on 13 January 2024.

data. In his 2024 speech Mr Ondrek Simej[68] also pointed out that Kenya would gain access to research, digital export services, Europe's growing data economy which is projected to be worth 800 billion euro by 2025, as well as various other benefits.[69]

On its own, the East African Community (EAC) is also taking steps towards harmonizing data governance through the Eastern Africa Regional Digital Integration Project. Considering these developments, it is important to ensure that the data that will be collected, processed and shared across various regions is collected in a manner that safeguards the privacy of all the citizens who will act as data subjects.

3.2 Current legal alternatives to 'legitimate interests'.

In Kenya, the DPA recognizes these lawful bases that a data controller or processor may rely upon to process personal data; First, under section 30(1)(a), data processing is lawful where the data subject consents to it for one or more specified purposes. Section 30(1)(b) states that processing may also be allowed when it is necessary for; performance of a contract, for compliance with any legal obligation for which the controller is subject, to protect the vital interests of the data subject or another natural person, to perform a task in the public interest, to perform a task carried out by the public authority, for legitimate interest pursued by the controller and for the purpose of historical, statistical, journalistic, literature and art or scientific research. [70]

Despite the fact that consent is mentioned as the first ground for processing data and there is use of the word 'or' before a separate listing of the other grounds of processing personal data, there is said to be no hierarchy among the grounds and neither one holds greater weight than another. Therefore, data controllers or processors are encouraged to use the one this is most appropriate to their activities.

3.3 Challenges and shortcomings of these alternatives:

3.3.1 CONSENT

Consent has conventionally been granted the most attention out of these grounds. This may be because on the surface, it seems to be the most straight forward one. One party asks if they may collect data for certain purposes and the other party allows them to do so. Even so, consent is also viewed by some as being too cumbersome, especially when dealing with a large number of customers which is why the 'legitimate interests' ground is often used.

---

[68] The currrent,2024, European Union Delegation to Kenya Charge d'affairs.

[69] Opening remarks by European Union Deputy Ambassador Ondrej Šimek at the Network for African Data Protection Authorities (NADPA) Conference , 7 May 2024 <https://www.eeas.europa.eu/delegations/kenya/opening-remarks-european-union-deputy-ambassador-ondrej-%C5%A1imek-network-african-data-protection_en?s=352 > on 13 January 2024.

[70] Section 30, Data Protection Act 2019.

Consent in the Kenyan DPA as well as the GDPR, has several conditions for it to have been validly collected. Consent must be freely given, unequivocal, express, specific, unambiguous and informed. In both instances, it must be collected through a statement or a clear affirmative action which indicated the data subject's agreement to have their data collected in this manner.[71] The EU directive 2016/679 gives further elaboration that silence, inactivity or pre ticked boxes are not proper ways of collecting consent.

This was emphasized in the *Orange Romania* case where Orange Romania, a mobile telecommunications provider, was acquiring consent using pre-ticked boxes which customers then had to sign to use their services. The contracts stated that the customers had been informed that the company would keep a record of their identity documents and had consented to the same. [72] Several problems were identified with this method of consent in that even though the company stated that they would still contract with people who did not give their consent, those people would have to get a separate form to fill in which created a higher burden for them. Moreover, there was no explanation of how this data would be used and how long it would be stored thus violating the requirement that consent should be informed. [73]

As demonstrated above, consent is a particularly stringent ground for data processing and the burden of proof for the collection of such consent is placed upon the data controller or processor.[74] It is not enough for the data controller to only meet one qualification for consent. If the consent is expressly given, either by signature or by a clear affirmative action, but it is not specific then consent is still deemed to have been improperly given. The specificity requirement is in line with the purpose limitation principle in that, when data is being collected there is a need to clearly outline what the data is going to be used for. Even once the data is already in the controller's possession, if the purpose for processing changes, then new consent must be collected.[75]

In the context of informed consent, such information is meant to be given in a manner that is easy to understand. This is contrary to the current norm of certain websites and some social media platforms which 'bury' their request for consent under lengthy terms and conditions which are often full of jargon and hard to understand.[76] Consent must also be freely given and unequivocal and this is especially important where there is a clear imbalance between the data subject and the data controller. A service provider who provides a service that is widely used such as TikTok or Facebook cannot condition the use of their application or service on receiving consent to process people's data in certain ways. This was outlined in the *Meta v Bundeskartellamt* case where it was

[71] Section 2 Kenya Data Protection Act 2019

[72] Orange Romania SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (2020), Court of Justice of the European Union.

[73] Orange Romania SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (2020), Court of Justice of the European Union,.

[74] Section 32(1) Data Protection Act Kenya,2019

[75] Section 6(5), The Data Pprotection (generall) Regulations, 2021.

[76] Section 4(b), The Data Pprotection (generall) Regulations, 2021.

stated that if there is no genuine or free choice or if consent cannot be withdrawn without detriment, then such consent is not freely given; consent was therefore not valid if it was a condition for using the social network.[77] The case also outlined that if there were separate data processing activities, consent must be taken for each one separately.[78]

A similar holding was made by the Kenyan ODPC when the Worldcoin project was undertaken in 2023. The project involved downloading an application. Before the users could use the application, there was a manual consent form which they would fill in. Moreover, they had to scan their irises to receive a digital ID and digital tokens worth KSH 7,000. Personal data such as their gender, facial image, phone number and a person's contacts were among the collected information. The consent obtained in this case was invalidated by the fact that for a person to obtain the token they had to consent to the collection and processing of their biometric data which undermined their free will. [79]

The requirements for consent, as demonstrated above, are currently the most elaborate and have been adequately expounded on within written legislation and in case law. The other data processing grounds have varying levels of certainty.

3.3.2 Necessity for performance of a contract

The next data protection ground is the necessity of processing personal data for the performance of a contract. The guidelines by the European Data Protection Board (EDPB) provide the most comprehensive insight on this ground. A data controller would have to prove that a valid contract exists and that, objectively, such processing is essential for the performance of the contract. [80] A mere mention of data processing within a contract does not prove that processing of personal data

[77] Meta Platforms Inc v Bundeskartellamt (2023), Court of Justice of the European Union.
[78] Meta Platforms Inc v Bundeskartellamt (2023), Court of Justice of the European Union.

[79] When Yes means No – A Look at Kenya's evolving Data Protection Framework 29 January 2024 https://aln.africa/insight/when-yes-means-no-a-look-at-kenyas-evolving-data-protection-framework/ on 8 January 2025

[80] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects 8 October 2019 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

is necessary and the failure to mention data processing in a contract does not mean that processing of data is not necessary for performance.[81]

Notably, the consent and necessity ground have a special relationship in that, a service provider should not rely on consent and thereafter state that collection of certain types of data is crucial to the provision of a service. If they cannot prove that completion of the contract would be impossible without this data, then this would negate the concept of freely given consent. In this sense, the two grounds cannot be relied on at the same time unless they can prove that without certain information, they would be unable to complete their end of the bargain then they cannot rely on this ground. It would then be easier for an online store to claim that without a customer's phone number, address or current location and name they would be unable to deliver the requested goods than it would be for Instagram to claim that they need this, or any sensitive personal data in order to provide its services. Even though the service provider would likely still obtain consent from consumers, perhaps by asking the for this information rather than simply collecting it based on information available online for example, the main ground for processing would not be consent.

3.3.3 Protection of the Vital interests of the data subject

The next alternative to 'legitimate interests' is when the processing in question is important for the 'vital interests' of the data subject or any natural person.[82] In the Kenyan context as well as in the EU's understanding of this ground, this can only be relied upon in times of emergencies.[83] Such situations are usually matters of life and death or at the very least, situations where a serious risk of injury is posed on a person or third party.[84] In these cases, data may be shared and collected to save life, for example. Where there is an unconscious patient who is unable to consent to the sharing or sensitive personal data such as their ordinary health status or religion (in the case where

---

[81] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects 8 October 2019 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

[82] Section 30, Data Protection Act 2019

[83] 'Kenya: Permitted processing of personal data', Rödl &Partner 14 March 2023. https://www.roedl.com/insights/kenya-processing-personal-data-legal-obligations#:~:text=Vital%20Interest&text=The%20processing%20of%20personal%20data%20is%20regarded%20as%20lawful%20where,that%20of%20another%20natural%20person.

[84] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC 9 April 2014 <https://www.dataprotection.ro/servlet/ViewDocument?id=1086 > on 15 January 2024.

a blood transfusion may be an option, religion of the patient may be important since Jehovah Witnesses for example, deem blood transfusions to be against divine law).[85]

The performance of a task carried out by a public authority or that which is carried out in the official authority granted to a data controller, is another legal ground for processing personal data. An example of this ground being applicable would be in situations such as the collection of personal data for the purpose of granting an individual an identity card. It may also be applicable in context of law enforcement where there is need to protect against fraud or illegal content being shared on the internet.[86] The other ground includes the processing of data for research, journalism, statistical or literature and artistic purposes.[87]

3.4 Conclusion

Interestingly, all the grounds except consent are said to require a necessity test. [88] While this may be true, I posit that since the other grounds are more certain than the necessity test is both easier to do and is more likely to result in a fair outcome. These grounds, with the exclusion of legitimate interests have a predetermined purpose and so the question becomes; is it necessary to collect geographical data or data concerning one's family to facilitate the performance of a contract or to protect the vital interests of a data subject?

These alternatives offer better safeguards given their certainty. With the current developments in the realm of regional data protection both within Africa and with the European Union, the current lack of specificity in this ground will only create challenges in the future some of which may involve irreparable damage, especially with the growing involvement of AI. These technologies tend to learn based of patterns and repetition and create patterns of their own which may inadvertently cause them to form biases and to profile certain people. in the Philippines, 'legitimate interests' is not deemed to be a lawful data processing ground where sensitive personal data is involved. [89] Such stringent measures should be considered in Kenya and for the upcoming regional framework in East Africa. Additionally, the Dutch Data Protection Authority argued that purely

---

[85] Patrini C, 'Ethical and legal aspects of refusal of blood transfusions by Jehovah's Witnesses, with particular reference to Italy' 12 January 2014 https://pmc.ncbi.nlm.nih.gov/articles/PMC3934270/#:~:text=However%2C%20it%20was%20not%20until,are%20contrary%20to%20divine%20law. On 16 January 2024.

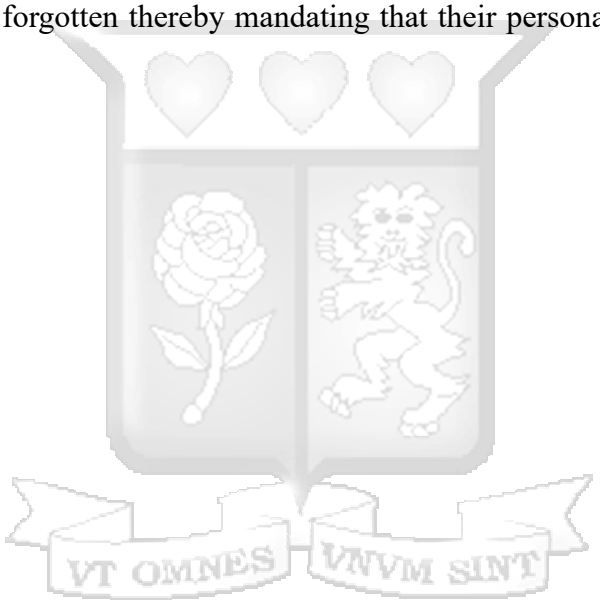
[86] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC 9 April 2014 < https://www.dataprotection.ro/servlet/ViewDocument?id=1086 > on 15 January 2024.

[87] Section 30,data protection Act, 2019.

[88] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC 9 April 2014,11 < https://www.dataprotection.ro/servlet/ViewDocument?id=1086 > on 15 January 2024.

[89] Circular on Guidelines for Legitimate Interest, Philippines, HYPERLINK "https://privacy.gov.ph/wp-content/uploads/2024/01/FAQ-Guidelines-on-Legitimate-Interest-as-of-28-December-2023.pdf"https://privacy.gov.ph/wp-content/uploads/2024/01/FAQ-Guidelines-on-Legitimate-Interest-as-of-28-December-2023.pdf on 11 January 2024.

commercial interests or profit maximization are neither specific enough nor do they have the character of a pressing lawful need.[90] This position should be applied in Kenya and in the upcoming regional frameworks such that, parties with commercial interests as their purpose for collecting data should rely on properly obtained consent from the data subjects. One parties' desire to make money should not reduce citizens to commodities in the sense that they are simply data points to be collected, analysed and whose information is traded to the highest bidder especially when this is not for their benefit. This goes against the universally agreed upon principle of human dignity and it is important to remember that there are several dangers that come from amassing the sensitive personal data of numerous people especially when they are unaware of how this data is collected, how much of it is collected and retained and for how long. Additionally, with the power imbalance between most citizens and the technological giants who tend to amass data in using the legitimate interest ground, they are often unaware that they have the power to object to processing as well as the right to be forgotten thereby mandating that their personal data should be deleted from servers.



[90]Gerritsen J, 'Administrative Court Judgment on the Interpretation of Commercial Interests as Legitimate Interests', 7(2), *European Data Protection Law Review*, 2021, 243.

4.0 CHAPTER FOUR: RECOMMENDATIONS AND CONCLUSION.

4.1 Introduction

In Kenya, there is a steady move towards digitizing services both in the private sector and those by government.[91] Data privacy and protection is therefore a topic which is increasingly gaining relevance as technology continues to outpace the laws that are meant to govern it. This is not an indication that legislators should bow down to the perceived inevitability of the laws they make becoming redundant with the innovation that is occurring. In fact, law makers should take up the challenge by learning more about the ins and outs of data collection and processing because one can only hope to control something that they at least moderately understand. Moreover, I believe that in this case it is better to err on the path of caution by attempting to regulate matters of data privacy as much as possible. With this in mind, gaps such as the ambiguity of the 'legitimate interest' data processing ground should not be overlooked.

4.2 Re-evaluating the theoretical understanding of legitimate interests :

As we move towards redefining what 'legitimate interests' means in the context of data privacy, who can rely on it and what the limits are for its application, we need to ensure that the burden of protecting personal data is not unfairly placed at the data subject's doorstep. The data subject currently seems to have the most amount of responsibility as they have to take measures to find out whether their data is being infringed by any service provider they come across. They then have to object to the processing and request for deletion of their personal data and hope that the data controller or data processor in question grants their request. While this may seem acceptable to some people who may argue that in any case, it is the data subject who has the most to lose and therefore they should take the lead in safeguarding their data, I do not agree with that view. In my opinion, such a viewpoint would not be applicable to other rights. If someone were to propose that the right to provision of the right to life meant that people should begin to wear bullet proof vests

[91] Kageni M and Odhiambo Y, 'Strengthening Data Protection in Kenya: Opportunities and the Way Forward' Kenya Institute Private Policy Research and Analysis, 30 June 2024.
https://kippra.or.ke/strengthening-data-protection-in-kenya-opportunities-and-the-way-forward/

in order to protect their right rather than ensuring that guns were not readily available, such a proposal would not be viewed as sound or acceptable.

When a right is granted, it should not be up to the right holder to constantly look over their shoulder to ensure that their rights are protected. Individuals should then have recourse in case their rights are infringed but the conditions that threaten their rights should be addressed and controlled first. In this context, the data controller who has the most to gain also enjoys the element of control in that, they will collect the data that they need or want and also be the ones to decide whether there is a high risk of infringing on data privacy. If they do determine that such high risk exists, they still have the authority to conduct the three-tier test and eventually determine whether their interests override the rights and interests of the data subjects. Additionally, even in the case where an individual or group of individuals becomes aware of data processing under the 'legitimate interests' ground that unfairly infringes on their rights, if they only choose to object to processing and do not take the initiative to report the entity then the other data subjects whose data is being processed in the same way but who remain ignorant, perhaps due to a lack of expertise in data related subjects, would still suffer from infringement.

4.3 A modification in the use of ‘legitimate interest’ ground.

The ‘'legitimate interests'’ ground seems to be more viable as a secondary step rather than as a data processing ground on its own. Treatment of this ground in such a manner would further the goals of data protection. By creating a two-tier system for data processing, especially when the initial tier is based on consent, there would be much more certain assurance for the protection of personal data. With this system, data controllers would first have to use any of the other grounds for processing personal data such as consent or for research purposes. Then the 'legitimate interests' test would come into play to help determine whether the data that has been collected for research is legitimate in that it does not unfairly intrude into the privacy of certain individuals. Even where consent has been collected, it is important for data controllers to still demonstrate that their use of data does not infringe on the data subjects' rights and interests.

Even so, there would still be a need to define what interests of the data subject are to be taken into account and whether the rights in question are only privacy rights or whether manipulation of

autonomy and choice is to be considered. Moreover, would interests such as avoidance of profiling and surveillance be included and what is the weight of these interests? Do they vary depending on the number of people involved, the amount of data collected or even the sophistication of the systems or AI processing the data? Of course, legislation cannot address every eventuality, especially in a dynamic sector such as the world of technology. However, foreseeable questions such as these should be addressed without having to wait for courts to grapple with them after a serious breach of right has occurred.

Alternatively, having a better funded office of the data commissioner with a department for officers knowledgeable in computer programming and related fields may be useful in that, where there are data controllers who handle large amounts of data, these officers may be involved in the assessment of whether the data being collected indeed is indeed in the legitimate interest of the prescribed purpose. While one must take cognizance of the fact that this measure may seem overly idealistic or too prescriptive, it is important to note that the involvement of these officers would not be a recurring procedure. They would ensure that the data collection, within firms that collect large amounts of data, is in line with the 'legitimate interests' they claim to have, and they would help data controllers in their assessment of whether their interests override the rights and interests of data subjects and more importantly, they would be neutral third parties who would be able to make the assessment without undue consideration to business interests.

4.4 Separate measures for the proper implementation of the current understanding of ‘legitimate interests’

Overall, there needs to be more effort in educating the public about their rights under the Data Protection Act. This is especially in relation to rights such as the right to object to processing of their personal data and the right to be forgotten. If citizens are to be able to play their role in safeguarding their data, they need to know what avenues are available to them.

Currently, there are efforts that are being made in creating regional data regulation frameworks. Some of the aims of this include; protecting citizens’ ‘digital rights, preventing abuse by big tech companies as well as facilitating cross border digital trade. With a united regional approach to data

regulation and protection, the hope is that the region's bargaining power will be strengthened especially when dealing with against technological giants such as Google and Meta. If this succeeds, it is important that the present ambiguity is not maintained in the new regulation that comes up.

Finally, one potentially effective approach, which Kenya has tried to do, or is perhaps in the process of implementing, is defining 'legitimate interests' based on context specific areas. What is legitimate processing of data in the communications sector could be different from the online banking sector and it is important to make these delineations. Such provisions would account for the nuanced needs of each sector based on the data needed to provide the specific services.

4.5 CONCLUSION:

In a world where data is increasingly becoming a vital resource for most businesses and organizations, especially those that are based online, this study has sought to shed light on a topic that seems too easily overlooked despite the risk of misuse. It has pointed out the need for greater discourse surrounding the 'legitimate interests' ground not just in the Kenyan context but globally. In any case, with the ongoing initiatives, cross-border data flows across various jurisdictions will only keep increasing. For the ongoing initiatives in Africa, they have all stated that their goals include safeguarding privacy while making it easier to transfer data across various regions. However, to properly safeguard privacy there is a need to ensure that from the initial collection of data, there is a well set out parameter for what ‘'legitimate interests'’ means and when it can be relied upon in sector specific areas. Its effective use should not be hindered by uncertainty.