Strathmore University

Law School

REGULATING SOCIAL MEDIA FOR KENYAN DEMOCRACY

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

Strathmore University Law School

By

[Njau Lucy Murugi]

[135143]

Prepared under the supervision of

[Mr. Cecil Abungu]

[February 2024]

Word count: 13,985

TABLE OF CONTENTS

Acknowledgments

I would like to extend my sincere gratitude to my supportive supervisor, Mr. Cecil Abungu. I am extremely grateful for his guidance, feedback, as well as friendly chats at the end of our meetings.

I am also deeply thankful to Esther Nyabuto and Janet Njau for consistently making time to review my dissertation and providing important feedback when needed. Their support throughout the project is greatly appreciated and has contributed significantly to the refinement of this dissertation.

A special acknowledgement goes to Regina Njau, who had to listen to me incessantly drone on about this dissertation all year long but still listened and never stopped encouraging me. Those phone calls in the middle of the day really did help me make it through it.

Finally, I would like to express my gratitude to my parents for their unwavering support during this project, which is the pinnacle of four years of learning. Without your support, I would have stopped these studies a long time ago. You have been amazing, and as promised, I will now clear all the papers off the dining table!

Dedication

For my younger self, who never imagined making it this far.

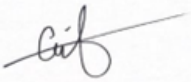
Declaration

I, **NJAU LUCY MURUGI**, 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 or referred to are accordingly acknowledged.

Signed: .....

Date: 16 February 2024

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



Signed: .....

[Cecil Abungu]

Abstract

In our digitally interconnected world, online political micro-targeting (OPM) presents both a promising avenue for engaging the electorate and a potential threat to the very fabric of democracy. This study, spurred by the prevalent use of OPM in Kenyan politics, has undertaken a comprehensive exploration of its impact, risks, and the inadequacies of existing regulatory frameworks. The primary focus has been on assessing the threat posed by OPM and developing a framework for its regulation.

Grounded in a qualitative methodological approach, the study relies mainly on secondary sources, including books, and articles. However, primary sources such as the Constitution of Kenya, the Data Protection Act, and the Computer Misuse and Cybercrimes Act are still utilised. It follows a deductive logic structure, using the findings in chapters two and three to validate the necessity for specialized legislation. Chapter two identifies gaps in current laws that fail to curb the risks associated with OPM, while chapter three evaluates international regulatory models to identify practices that could be adapted to the Kenyan context.

Chapter four then delivers the crux of the argument: Kenya's democracy urgently requires specialized legislation to address OPM. The recommended legal approach—'the information control approach' - envisions an effective regulatory environment where misinformation is proactively eliminated, and transparent measures are put in place. This proposed legislation aims at strengthening the electoral process by ensuring that social media platforms adhere to stringent criteria, instituting penalties to deter OPM abuses.

.

List of Abbreviations

ABA	Attribute-based Audiences technology
CMCA	Computer Misuse and Cybercrimes Act
DPA	Data Protection Act
KANU	Kenya African National Union
KPU	Kenya People's Union
OPM	Online Political Microtargeting
PII	Personally Identifying Information Audiences technology

List of Cases

Kenya

Jacqueline Okuta and another v Attorney General and 2 others (2017) eKLR.

United States of America

Stratton Oakmont, Inc. v Prodigy Services Co. (1995), New York Supreme Court.

List of Legal Instruments

Kenya

Computer Misuse and Cybercrimes Act (2018).

Constitution of Kenya (2010).

Data Protection Act (2019).

Data Protection Act Policy (2018).

Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules (2021).

Canada

Elections Modernization Act (Canada).

France

Code electoral (France).

Germany

Network Enforcement Act (Germany).

Singapore

Code of Practice for Transparency of Online Political Advertisement (Singapore).

United States of America

Communications Decency Act (United States of America).

1.0 INTRODUCTION

1.1 Background

According to a study by Statista, a fifth of Kenyans are registered on at least one social media platform.[1] These Kenyans spend, on average, two hours daily mindlessly scrolling, liking and sharing posts on various platform(s).[2] The platforms then collect this data using electronic tools, such as 'Cookies', and either use it for microtargeting or sell it to third parties to use it for microtargeting.[3] Microtargeting is a technique that utilises demographics and consumer data to identify and influence the thoughts or actions of specific people or very small groups of like- minded individuals.[4] When used as a marketing tool, it can be considered a legitimate next-generation tool which allows organisations to target a receptive audience without wasting its resources engaging with those who are unlikely to be interested.[5]

However, when used in the political sphere, micro-targeting may undermine democracy. Before we delve into why, it is important to understand what Online Political Micro-targeting (OPM) entails. This practice, utilised by political campaigns, leverages detailed data profiles and algorithms to send targeted content to citizens.[6] Thus, using OPM, political parties can identify the specific voters they are most likely to persuade and tailor their messages to their interests and weaknesses.[7]

The reason why OPM is inherently more problematic to democracy, as opposed to traditional forms of political campaigning, stems from its utilisation of filter bubbles and fake news. The term "Filter Bubbles" describes a scenario wherein social media platforms employ personalised content selection algorithms to tailor content according to an individual's preferences and past behaviours. This then creates a bubble around

---

[1] Statista, *Number of social media users in Kenya from 2014 to 2022*, 1 Aug 2022, 1.
[2] Wamuyu P, 'Social Media Consumption Among Kenyans: Trends and Practices' *IGI Global,* 2020, 23-https://doi.org/10.4018/978-1-7998-4718-2.ch006 on 13 January 2023.
[3] Frederik J, Zuiderveen B, Möller J, Kruikemeier S, Fathaigh R, Irion K, Dobber T, Bodo B, and Vreese C, 'Online Political Microtargeting: Promises and Threats for Democracy' *Utrecht Law Review,* 2018, 84.
[4] Mude H, 'Political Micro-Targeting in Kenya: An Analysis of the Legality of Data Driven Campaign Strategies under the Data Protection Act' 1 *Journal of Intellectual Property and Information Technology Law* 1, 2021, 7.
[5] <https://insights.advocates.ke/legal-reforms-kenya-can-borrow-to-regulate-microtargeting/> on 13 Janury 2023.
[6] Bulka T, 'Algorithms and Misinformation: The Constitutional Implications of Regulating Microtargeting' 32 *Fordham Intellectual Property, Media and Entertainment Law Journal* 4, 2022, 1112.
[7] Frederik J, Zuiderveen B, Möller J, Kruikemeier S, Fathaigh R, Irion K, Dobber T, Bodo B, and Vreese C, 'Online Political Microtargeting: Promises and Threats for De mocracy,' 86.

individuals, where they are exposed to a narrow range of content, reinforcing their pre-existing beliefs and limiting exposure to alternative viewpoints.[8] Filter bubbles pose a threat to democracy as they contribute to the formation of echo chambers, where individuals are exposed to only information they want to hear rather than what they need to hear for a well-rounded understanding of political issues- and since these filters are invisible, people do not know what is being hidden from them.[9] In contrast, traditional political campaigning methods lack the capacity to generate filter bubbles as they operate on a broadcast model, which has limited personalisation.[10]

Fake news, characterised by false information, has the potential to significantly mislead readers.[11] During political campaigning, this is a strategic tool to target individuals or groups by capitalising on existing beliefs and vulnerabilities.[12] This manipulative tactic takes advantage of filter bubbles thus distorting an individual's understanding of reality and swaying public opinion. Furthermore, the viral tendency of fake news in online ecosystems, facilitated by the interconnectedness of social media platforms, amplifies its impact.[13] This is unlike traditional campaign methods, where news spreads at a comparatively slower pace.[14]

These intrinsic features of OPM, while detrimental to democracy, prove highly advantageous for political campaigning endeavours.[15] Consequently, numerous instances of its application have emerged globally. For example, in the United States of America (USA), Cambridge Analytica, a controversial data analytics firm, utilised 87 million people's personal data to influence politics through OPM, thus undermining democracy.[16] Similarly, during the Brexit campaign in the United Kingdom, OPM was employed by the Vote Leave campaign. The campaign targeted vulnerable voters with fake news, using

[8] Flaxman S, Goel S, and Rao J, 'Filter Bubbles, Echo Chambers, and Online News Consumption' 80 *Public Opinion Quarterly* 1, 2016, 301.
[9] Pariser E, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think,* Penguin Publishing Group, London, 2011, 10.
[10] Flaxman S, Goel S, and Rao J, 'Filter Bubbles, Echo Chambers, and Online News Consumption,' 307.
[11] Allcott H and Gentzkow M, 'Social Media and Fake News in the 2016 Election' *31 Journal of Economic Perspectives* 2, 2017, 213.
[12] Yerlikaya T and Aslan S, 'Social Media and Fake News in the Post-Truth Era: The Manipulation of Politics in the Election Process' 22 *Insight Turkey* 2, 2020, 180.
[13] Farkas J, 'Fake News in Metajournalistic Discourse' 24 *Journalism Studies* 4, 2023, 426.
[14] Morozov E, *The Net Delusion: The Dark Side of Internet Freedom,* PublicAffairs Books, New York, 2014, 244.
[15] Morozov E, *The Net Delusion: The Dark Side of Internet Freedom*, 264.
[16] Granville K, 'Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens' The New York Times, 4 April 2018—<https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html > on 13 January 2023.

microtargeting to ensure that these messages reached the people who were most likely to be influenced by them.[17]

In response to this, numerous countries in the Global North have since passed legislation to regulate social media platforms, mandating them to adhere to stringent accountability and transparency standards when it comes to OPM.[18] The aim is to prevent the recurrence of such incidents and safeguard democratic processes in their respective nations.

In Kenya, data-driven campaigning and its ramifications to the functioning of a democracy have been assumed to be an issue of the Global North solely,[19] with some scholars even remarking that no sophisticated algorithm or complex figure crunching is going to have an impact on the country's ethnic-based politics.[20] Other scholars opine that regulation is unnecessary since most political parties lack the skills necessary to conduct a successful microtargeting campaign, resulting in a "gulf between the rhetoric and reality of data driven campaigning".[21] This was until the general elections of 2013 and 2017 where the major political parties were accused of using OPM.[22] The Jubilee Party, for instance, hired the infamous Cambridge Analytica, to 'assist with branding,' but later investigative journalism showed that this was an understatement as they were reported to have profiled and micro-targeted voters based on their fears and desires.[23] Furthermore, there was also the use of OPM by Harris Media LLC where they circulated two aggressive videos, *The Real Raila* and *Uhuru for Us,* on social media that capitalised on Kenya's violent history to instil fear amongst voters, with *The Real Raila* campaign asserting that the opposition candidate's presidency would "eliminate whole tribes".[24]

---

[17] Vote Leave's targeted Brexit ads released by Facebook' BBC News, 26 July 2018 – <https://www.bbc.com/news/uk-politics-44966969> on 15 April 2023.
[18] Examples include: Canada's Elections Modernization Act (2018), Singapore's Code of Practice for Transparency of Online Political Advertisement (2019), and France's Electoral Code in Article L 163-1.
[19] Mude H, 'Political Micro-Targeting in Kenya: An Analysis of the Legality of Data Driven Campaign Strategies under the Data Protection Act,' 9.
[20] Mude H, 'Political Micro-Targeting in Kenya: An Analysis of the Legality of Data Driven Campaign Strategies under the Data Protection Act,' 9.
[21] Dommett K, 'Data-driven political campaigns in practice: understanding and regulating diverse data-driven campaigns' 8 *Internet Policy Review* 4, 2019, 8.
[22] Muthuri R, Karanja M, Monyango F and Karanja W, 'Investigating privacy implications of biometric voter registration In Kenya's 2017 election Process' 1 *Centre for Intellectual Property and Information Technology Law* 1, 2018.
Mutung'u, G, 'The Influence Industry Data and Digital Election Campaigning in Kenya' 1 *Our Data Ourselves* 1, 2018, 12.
[23] Dommett K, 'Data-driven political campaigns in practice: understanding and regulating diverse data-driven campaigns,' 11.
[24] Dommett K, 'Data-driven political campaigns in practice: understanding and regulating diverse data-driven campaigns,' 13.

Despite this, social media platforms are still allowed to practise OPM or sell their users' information to third parties or political parties, who then use it for OPM. This is because there is currently no comprehensive legislative framework that governs social media platforms or even just OPM. There are only laws which have provisions that may be applicable to OPM practices such as the Computer Misuse and Cybercrimes Act, and the Data Protection Act.

1.2 Problem Statement

Currently, the law in Kenya permits social media platforms to engage in OPM and sell user data to third parties, including political parties practising OPM. OPM has the potential to undermine democracy, as evidenced by its impact during the 2013 and 2017 general elections. However, there is currently no comprehensive legislative framework governing social media platforms or OPM. Only existing laws, such as the Computer Misuse and Cybercrimes Act, and the Data Protection Act, contain provisions that may relate to microtargeting practices. This study aims to evaluate whether the government of Kenya should introduce laws to regulate social media platforms to prevent OPM from destabilising democracy. If regulation is deemed necessary, the study will also explore what approach such laws should take to effectively address the challenges posed by OPM.

1.3 Research Questions

1. a) What is OPM, and what risks does it pose in a democracy?

   b) Is existing law enough to regulate OPM?

2. Globally, what are the current approaches to regulating OPM, and what are the merits and demerits of such approaches?

3. Should Kenya have specialised law to regulate OPM, and, if so, what approach should it take?

1.4 Research Objectives

1. To demonstrate how OPM works, the various ways it undermines democracy, and assess the adequacy of current regulations in Kenya in regulating OPM.

2. To examine the three regulatory approaches taken by other jurisdictions when regulating OPM and determine their merits and demerits.

3. To assess whether Kenya should adopt specialised laws to regulate OPM and, if so, determine the appropriate regulatory approach considering its specific contextual circumstances.

1.5 Justification

This study is crucial in Kenya, where the use of OPM as a campaign strategy poses a threat to election integrity, despite current regulations not addressing this risk. Unlike earlier academic literature on microtargeting, this analysis focuses solely on OPM, demonstrating regulatory shortcomings and proposing effective solutions. The findings of this study will be useful to lawmakers as it offers a roadmap for addressing legislative deficiencies. Moreover, scholars examining the intersection of technology, politics, and democracy can benefit from research into how social media platforms are utilised for political purposes. Finally, civil society organisations, concerned with democracy, good governance, and digital rights, like the Council for Responsible Social Media in Kenya, may gain an understanding about the impact of OPM on democratic processes and the role of regulating social media platforms in addressing these issues.

1.6 Conceptual Framework: Social Media as a Public Utility

Social media has become an integral element of modern life, with billions of people utilising platforms such as Instagram, Facebook, YouTube, and Twitter on a daily basis.[25] While these platforms were initially intended to connect friends and families, they have now evolved into powerful tools for communication, cooperation, and information exchange.[26] Due to this evolution, social media platforms have now become a public utility and this concept aims to depict this. To do this, it will begin by describing what public utilities are. Then, it will illustrate how social media platforms fit within this definition. Finally, it will examine the potential implications of this designation.

A public utility is a service or commodity that is critical to public welfare and should thus be provided by the government or be subject to stringent government regulation to ensure

[25] Global Web Index, Social Media Statistics, 2023, 2.
[26] Awad J and Krishnam M, 'Social Media and Its Role in Political Campaigns: A Review of Literature' *University of Pennsylvania Press*, 17 Aug 2020—< https://knowledge.wharton.upenn.edu/podcast/knowledge-at-wharton-podcast/how-social-media-is-shaping-political-campaigns/> on 3 March 2023.

that it is provided fairly, reliably, efficiently and affordably.[27] Examples of public utilities include electricity, telecommunications, water, and transportation.[28] The key characteristic of a public utility is that it offers a critical service or commodity that is required for the overall well-being of society.[29]

Social media platforms can be categorised as public utilities for three reasons:

Firstly, they serve as a crucial mode of communication for many people. These days, social media platforms are not only used to keep in touch with friends and family but also to share news, information, and ideas with a broader audience.[30] For many people, social media has largely supplanted conventional media channels as their major source of news and information.[31] This is particularly true for younger generations, who are more likely to gather their news from social media than from traditional news sources.[32] As a result of this dependency on social media - for communication and information exchange - it is becoming increasingly difficult for individuals to fully engage in society if they do not have access to these platforms. For instance, social media may be necessary when job hunting, keeping up with local events and politics, or campaigning for a cause.[33] In this regard, social media is analogous to other vital services, such as electricity or telephones, which are required for individuals to fully engage in society.

Secondly, social media has evolved into an essential instrument for social and political activity. It has played a major role in mobilising and organising people around critical social and political concerns, from the Arab Spring[34] to the Black Lives Matter campaign.[35] In many situations, social media has given disadvantaged people a forum to raise their voices and campaign for change.[36] Nevertheless, while social media is utilised for political organising and advocacy, it can equally be used for repression and censorship.

---

[27] Geddes R, 'Public Utilities' Cornell University, Working Paper, 1998, 4 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=92688 on 7 March 2023.
[28] Phillips C, 'The Regulation of Public Utilities' 2 *Technology and Investment Journal* 1, 2010, 96.
[29] Phillips C, 'The Regulation of Public Utilities,' 96.
[30] Sunstein C, *Republic: Divided Democracy in the Age of Social Media*, Princeton University Press, New Jersey, 2017, 97.
[31] University of Oxford, *The Reuters Institute Digital News Report,* 2021, 4.
[32] University of Oxford, *The Reuters Institute Digital News Report,* 2021, 4.
[33] Sunstein C, *Republic: Divided Democracy in the Age of Social Media*, 97.
[34] Tufekci Z, 'Twitter and Tear Gas: The Power and Fragility of Networked' 38 *Strategic Studies* 3, 2018, 114.
[35] Tufekci Z, 'Twitter and Tear Gas: The Power and Fragility of Networked,' 114.
[36] Ghonim W, *Revolution 2.0: The Power of the People Is Greater Than the People in Power: A Memoir*, Houghton Mifflin Harcourt, Egypt, 2012, 111.

Globally, governments have utilised social media to monitor and suppress political protests, and social media platforms have been chastised for their involvement in supporting such repression.[37] Recognising the potential for social media to be used for both social and political organising, as well as repression, emphasises the importance of viewing social media as a public utility. Consequently, legislative control is needed to ensure its utilisation in accordance with democratic principles and human rights.

Thirdly, social media has evolved into an essential tool for gathering and disseminating information. Individuals now have access a broad diversity of information and ideas from all over the world thanks to the growth of social media.[38] This has the ability to foster greater understanding and empathy among people of various cultures and origins. Nonetheless, increasing access to information means that people are frequently bombarded with large volumes of information, much of which may be inaccurate or misleading.[39] This can make it difficult for people to distinguish between reality and fiction and make educated judgements. Thus, government intervention is necessary to establish regulations that ensure the responsible use of social media and mitigate the risks associated with misinformation.

Having established how social media can be considered a public utility, it ought to be regulated to ensure that individuals are able to access accurate and reliable information.

1.7 Literature Review

So far, literature on OPM has mainly focused on microtargeting (as a whole rather than just OPM),[40] defining it,[41] discussing how it is a privacy issue,[42] debating whether it is a substantial threat to democracy,[43] discussing whether its justifiable to regulate social

[37] Amnesty International's report, *Tear Down This Wall: The Anatomy of Facebook's Role in the Myanmar Genocide*, 2020.
[38] Ghonim W, *Revolution 2.0: The Power of the People Is Greater Than the People in Power: A Memoir*, 111.
[39] Sunstein C, *Republic: Divided Democracy in the Age of Social Media*, 94.
[40] Mude H, 'Political Micro-Targeting in Kenya: An Analysis of the Legality of Data Driven Campaign Strategies under the Data Protection Act,' 22.
[41] Mude H, 'Political Micro-Targeting in Kenya: An Analysis of the Legality of Data Driven Campaign Strategies under the Data Protection Act,' 8.
[42] Monyango F, *Kenya: Overview of the Data Protection Act*, 2019.
Muthuri R, Karanja M, Monyango F and Karanja W, 'Investigating privacy implications of biometric voter registration In Kenya's 2017 election Process,' 13.
[43] Muthuri R, Karanja M, Monyango F and Karanja W, 'Investigating privacy implications of biometric voter registration In Kenya's 2017 election Process,' 19.

media platforms due to its presence,[44] and illustrating how present regulation, specifically the Data Protection Act, is sufficient to regulate all types of political microtargeting.[45] Although this research problem was touched upon in a blog post, the claim made there was presumptive and lacked sufficient detail.[46] Therefore, I expect that my study will offer a unique contribution by providing an in-depth analysis on why OPM remains an issue that is not adequately addressed by existing regulations and proposing the regulation of social media platforms as a necessary solution to prevent it.

1.7.1 On the Potential Democratic Risks of OPM Compared to Traditional Political Campaigning

Scholars worldwide have debated the potential democratic risks associated with OPM, leading to a diverse range of perspectives. Within this discourse, some scholars adopt a sceptical stance towards the potential negative impacts of OPM. For instance, Vold et al have opined that there is a temptation to oversell, overhype and catastrophize the effects of political micro-targeting.[47] Similarly, Dommett argues that most political parties lack the skills necessary to conduct a successful microtargeting campaign, resulting in a "gulf between the rhetoric and reality of data driven campaigning".[48]

Other scholars, however, have adopted a more moderate position providing that the effects of OPM on democratic outcomes are uncertain.[49] According to Nyhan, this is because OPM is simply the latest evolution of long-standing practices of political persuasion and messaging, and so its impact on democracy should not be overstated.[50] Similar conclusions have also been arrived at by other scholars who acknowledge that while OPM can have negative effects on political discourse and representation, it is not inherently a

[44] Dommett K, 'Data-driven political campaigns in practice: understanding and regulating diverse data-driven campaigns,' 24.
Rutenberg I and Sugow A, 'Regulation of the Social Media in Electoral Democracies: A Case of Kenya' 8 *Journal of African Law* 1, 2020, 7.
[45] Mude H, 'Political Micro-Targeting in Kenya: An Analysis of the Legality of Data Driven Campaign Strategies under the Data Protection Act,' 12.
[46] -<https://insights.advocates.ke/legal-reforms-kenya-can-borrow-to-regulate-microtargeting/> - on 13 January 2023.
[47] Vold K and Whittlestone J, 'Privacy, autonomy, and personalised targeting: rethinking how personal data is used' *Leverhulme Centre for the Future of Intelligence*, 2019, 6 - http://lcfi.ac.uk/resources/privacy-autonomy-and-personalised-targeting-rethin/ - on 13 January 2023.
[48] Dommett K, 'Data-driven political campaigns in practice: understanding and regulating diverse data-driven campaigns,' 18.
[49] Nyhan B and Reifler J, 'When corrections fail: The persistence of political misperceptions' 32 *Political Behavior* 2, 2010, 313.
[50] Nyhan B and Reifler J, 'When corrections fail: The persistence of political misperceptions,' 316.

threat to democracy.[51] Other factors such as media coverage and traditional campaigning tactics may be more important determinants of electoral success.[52]

In retaliation to this, some scholars have criticised these sceptics for being short-sighted, as political parties will not always be unable to conduct OPM, especially in the future. [53] Moreover, according to them, a legislator's mandate includes anticipating issues and intervening before they occur, rather than just waiting for them to occur.[54] They emphasise that harm does not have to occur in grand proportions to be addressed.

On the other end of the spectrum are scholars like Seth Flaxman et al, and Parisier, who adamantly assert that microtargeting is a great danger to democracy even in the present. This is attributed to its role in creating echo chambers - online environments in which people are exposed only to information that confirms and aligns with their existing beliefs. They argue that microtargeting facilitates the development of these echo chambers thus contributing to a breakdown in democratic discourse and making it easier for false information to spread.[55]

1.7.2 On Regulatory Approaches to Addressing OPM

In Kenya, scholars like Hashim Mude assert that the Data Protection Act is comprehensive enough to regulate microtargeting.[56] This perspective stems from the belief that microtargeting is primarily a privacy issue. Consequently, given that the Data Protection Act now requires consent to be provided prior to data collection, it is deemed sufficient to regulate microtargeting.[57]

Conversely, some scholars claim that current regulations are inadequate to address microtargeting, primarily due to the absence of tailored provisions for this emerging

[51] Hoegg J and Lewis M. 'The Impact of Candidate Appearance and Advertising Strategies on Election Results' 48 *Journal of Marketing Research* 5, 2011, 907.
[52] Hoegg J and Lewis M. 'The Impact of Candidate Appearance and Advertising Strategies on Election Results,' 908.
[53] Muthuri R, Karanja M, Monyango F and Karanja W, 'Investigating privacy implications of biometric voter registration In Kenya's 2017 election Process,' 22.
[54] Muthuri R, Karanja M, Monyango F and Karanja W, 'Investigating privacy implications of biometric voter registration In Kenya's 2017 election Process,' 22.
[55] Pariser, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*, 64.
Flaxman S, Goel S and Rao J, 'Filter Bubbles, Echo Chambers, and Online News Consumption,' 307.
[56] Mude H, 'Political Micro-Targeting in Kenya: An Analysis of the Legality of Data Driven Campaign Strategies under the Data Protection Act,' 9.
[57] Mude H, 'Political Micro-Targeting in Kenya: An Analysis of the Legality of Data Driven Campaign Strategies under the Data Protection Act,' 15.

practice.[58] However, they argue that addressing this gap does not necessitate additional legislation; instead, they propose that social media platforms should self-regulate.[59] The rationale for this approach is that it brings inherent advantages, such as fostering innovation within online communities. [60]

Other scholars who argue against government regulation mainly do so on the grounds that regulation would not only be difficult to enforce[61] but also could also have unintended consequences. For instance, they highlight it could infringe on a social media user's right to freedom of expression as was witnessed in Germany.[62]

In response to the scholars advocating for self-regulation, Leerssen et al and Jamieson shed light on the complexities associated with this approach.[63] They illustrate these complexities by examining how platforms like Facebook have chosen to regulate themselves. Facebook introduced transparency mechanisms to mitigate the negative impact of OPM. These mechanisms included publicly-searchable political ad libraries that make it more difficult to post 'dark ads' (messages only visible to targeted groups).[64] However, Leerson et al points out that the present implementations of these ad-libraries leave much to be desired. For instance, the definition of 'political' ads varies widely leading to uncertainty and challenges when it comes to enforcement.[65] Moreover, the question of whether and how platforms should ensure proper identification of ad buyers is still yet to be resolved, as the platform has still not provided information on how and to

[58] Dobber T, Fathaigh R and Borgesius F, 'The regulation of online political micro-targeting in Europe' 8 *Internet Policy Review* 4, 2019, 47.
Rutenberg I and Sugow A, 'Regulation of the Social Media in Electoral Democracies: A Case of Kenya,' 11.
[59] Rutenberg I and Sugow A, 'Regulation of the Social Media in Electoral Democracies: A Case of Kenya,' 39.
[60] Rutenberg I and Sugow A, 'Regulation of the Social Media in Electoral Democracies: A Case of Kenya,' 24.
[61] Article 19, *Germany: Responding to Hate Speech. Country Report*, 2018, 16.
[62] Tworek H and Leerssen P, 'An Analysis of Germany's NetzDG Law' University of Amsterdam, Transatlantic Working Group Working Paper, 2019, 8 https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Le on 10 January 2023.
[63] Leerssen P, Ausloos J, Zarouali B, Helberger N, and de Vreese C. H., 'Platform ad archives: promises and pitfalls' 8 *Internet Policy Review* 4, 2019, 6.
Jamieson K, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President—What We Don't, Can't, and Do Know,* Oxford University Press, New York, 2020, 88.
[64] https://www.facebook.com/business/news/bringing-more-transparency-to-political-ads-in-2019 in 2019.
[65] Leerssen P, Ausloos J, Zarouali B, Helberger N, and de Vreese H, 'Platform ad archives: promises and pitfalls,' 32.

whom political ads are targeted.[66]

Given the myriad of challenges that arise with self-regulation, scholars such as Dobber et al, have instead opted to advocate for a specialised law to regulate OPM.[6782] They suggest that countries should take inspiration from other countries like France, where the electoral code mandates that in the three months prior to elections, online platforms must provide users with information about the financiers of "promotion of content related to a debate of general interest".[68] Nevertheless, they recognise that these types of bans may not capture all forms of indirect political advertising. Instances still arise where ad campaigns refrain from explicit promotion of a particular party or candidate, despite the campaign's theme and message aligning with the particular party or candidate's agenda.[69] Despite these challenges, these scholars argue that while a specialised law might not be a panacea, it offers a more comprehensive approach compared to relying solely on self-regulation or interpreting data protection rules to govern the landscape of OPM.[70]

1.8 Contribution

So far, literature on OPM and its implications for democracy has primarily focused on describing OPM, assessing its potential risks, and debating the effectiveness of current regulations. In this context, my study makes a unique contribution by scrutinizing the shortcomings of the current regulatory framework in Kenya and proposing an approach to address these deficiencies. Thus, this research extends beyond existing discussions to offer practical solutions that consider the socio-economic context and challenges related to regulating OPM effectively.

1.9 Methodology

This study will consist of three major parts, each employing different methodologies to address the research objectives. The study will be qualitative in nature, and will mainly rely on secondary sources such as books, book chapters, journal articles, and other internet sources. Nevertheless, a few primary sources, including the Constitution of Kenya, the

[66] Leerssen P, Ausloos J, Zarouali B, Helberger N, and de Vreese H, 'Platform ad archives: promises and pitfalls,' 36.
Jamieson K, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President—What We Don't, Can't, and Do Know,* 91.
[67] Dobber T, Fathaigh R and Borgesius F, 'The regulation of online political micro-targeting in Europe,' 14.
[68] Article L 163-1, *France's Electoral Code* (France).
[69] Dobber T, Fathaigh R and Borgesius F, 'The regulation of online political micro-targeting in Europe,' 16.
[70] Dobber T, Fathaigh R and Borgesius F, 'The regulation of online political micro-targeting in Europe,' 19.

Data Protection Act and the Computer Misuse and Cybercrimes Act, will be consulted.

The study will utilise a deductive method to arrive at its hypothesis. The first two parts will establish the premise leading to the main claim, with the first part demonstrating that OPM is not sufficiently regulated, while the second part presents potential solutions for its regulation. This text will conclude by discussing why Kenya needs specialised law to regulate OPM before selecting the best option for Kenya in terms of regulation. This strategy will ensure clarity and fluency in the study's structure and argumentation.

The first part of the study, which aims to define OPM, comprehensively explore its adverse effects on democracy, and explain the shortcomings of current regulations in preventing these harms, will be achieved through a thorough review of existing literature. Thereafter, the study will conduct a doctrinal analysis to determine if the Data Protection Act, and the Computer Misuse and Cybercrimes Act protect against these harms.

In the second part of the study, a policy analysis will be conducted to examine the regulations implemented by other jurisdictions to counteract the effects of OPM. This analysis will categorise these regulatory approaches into three and discuss their respective merits and demerits.

Finally, the study will determine the most suitable approach for Kenya to use to regulate OPM. To do so, it will conduct a contextual analysis of Kenya's political scene to identify the most favourable regulatory approach.

1.10 Chapter Breakdown

Chapter one will act as an introduction to the study, providing a foundation for the subsequent chapters. It aims to establish the research questions and objectives, as well as the conceptual framework that will be utilised throughout the study. This chapter will play a crucial role in setting the context for the entire study and helping readers gain a better understanding of the purpose and scope of the study. Furthermore, it will serve as a guide for readers, enabling them to follow the progression of the study and interpret the results of the subsequent chapters in the proper perspective.

Chapter two sets out to describe what OPM is, how it works, and how, through its working, various harms to the democracy of a country manifest themselves. Thereafter, the chapter will illustrate how the Data Protection Act, and the Computer Misuse and Cybercrimes

Act do not offer adequate protection against the potential harms that OPM can cause to society.

Chapter three will assess the approaches different jurisdictions have taken when regulating OPM. To do so, it will group these approaches into three. The first approach advocates for an outright prohibition of the use of OPM for political advertisements on social media platforms. The second approach permits OPM but mandates social media platforms to delete all harmful and misleading information on their platforms. Finally, the third approach requires social media platforms to adhere to stringent disclosure requirements if they are to participate in the political microtargeting of users.

Chapter four aims to prove the study's hypothesis; that regulating social media platforms is necessary for Kenya if it is to prevent OPM from damaging democracy. The chapter will argue that Kenya needs specialised law to regulate OPM and will also propose the most suitable approach for this specialised law. Specifically, the information control approach, where social media platforms are required to delete all harmful information and adhere to a list of other specifications, will be advocated as the most appropriate for Kenya, considering its historical and contextual circumstances. This approach is expected not only to avert the adverse effects of OPM but also to align effectively with Kenya's distinct context.

Chapter five will conclude the study.

2.0 UNDERSTANDING HOW OPM WORKS, ITS RISKS IN A DEMOCRACY, AND THE INADEQUACY OF CURRENT REGULATION

2.1 Introduction

This chapter aims to illustrate the negative effects that OPM has on Kenyan democracy and highlight the inadequacy of current regulation in mitigating these effects. The chapter begins by explaining what OPM is, what it is not, and its benefits before delving into ways OPM can be used to undermine democracy. Following that, the chapter discusses instances in Kenya where OPM has been exploited to undermine democracy. The subsequent sections then analyse Kenyan law and identify its inadequacies in regulating OPM. This analysis focuses on key aspects of the Data Protection Act and the Computer Misuse and Cybercrimes Act, illustrating how they still allow for OPM and its adverse effects.

2.2 Understanding OPM

After reviewing the scholarly work surrounding OPM, one should begin by distinguishing between regular political targeting, political microtargeting, and online political microtargeting.

Regular political targeting refers to the traditional methods political parties use to gather information about voters' preferences.[71] These methods, such as door-to-door canvassing, enable political parties to collect information about a broad category of voters in a particular area, and customise their campaigns accordingly.[72]

Political Microtargeting (PM), on the other hand, takes into consideration audience heterogeneity. This implies it is considerably more customised and personalised.[73] In the context of Kenya, PM was used during the 2017 elections by Cambridge Analytica, a Big Data firm. This company acquired alphanumeric data, likely obtained from the voters' register, which included the voters' names and the polling station they were registered at.

[71] Mude H, 'Political Micro-Targeting in Kenya: An Analysis of the Legality of Data Driven Campaign Strategies under the Data Protection Act,' 7.
[72] Dommett K, 'Data-driven political campaigns in practice: understanding and regulating diverse data-driven campaigns,' 27.
[73] Dobber T, Fathaigh R and Borgesius F, 'The regulation of online political micro-targeting in Europe' 8 *Internet Policy Review* 4, 2019, 61.

Then, it used this information to send the voters personalised messages - with up to 22% of these messages addressing voters by their first names - to encourage voters to support a particular candidate.[74] Although this targeting method was not too complex, it was undeniably personalised. This can be attributed to the fact that Kenya's socio-ethnic background allows for political affiliations to be reasonably deduced from just two factors: a voter's name and voting location.[75] Thus, even if this information did not formally disclose an individual's political affiliations, its ability to act as a proxy for a person's political views qualified it as PM.

Alternatively, OPM is the use of highly detailed data profiles to feed individuals with political information. Through programmed algorithms, platforms automatically choose stories, posts, and/or videos that match a specific user's interests.[76] These selected posts are then prioritised at the top of the user's social media feed and search engine results. Thus, the accuracy of this algorithm increases with more input information.[77]

OPM differs from PM in three main ways. Firstly, as OPM is used only by social media platforms,[78] it is limited to online communication while PM can be used for both offline and online communication. Additionally, given OPM's extensive use by tech giants, it involves the use of much more detailed data profiles.[79] Platforms have access to much more personal information, such as an individual's zip code, gender and age, among other personal details.[80] Notably, these platforms are also able to analyse digital footprints, for example online written text, to predict a citizen's personality. This means that, through natural language processing and machine learning algorithms, these platforms are able to learn latent psychological traits of a citizen from their online text.[81] Consequently, the

[74] Muthuri R, Karanja M, Monyango F and Karanja W, 'Investigating privacy implications of biometric voter registration In Kenya's 2017 election Process,' 11.
[75] Wanyama F, Elkit J, Frederiksen B and Kaarsholm P, 'Ethnicity and/or Issues? The 2013 General Elections in Western Kenya' 13 *Journal of African Elections* 2, 2014, 13.
Andreassen BA, Barasa T, Kibua T and Tostensen A, "I acted under a lot of pressure": the Disputed Kenyan 2007 general election in context' NORDEM Report, 2008, 77.
[76] Benjamin S, 'The First Amendment and Algorithms' in Woodrow Barfield (ed) *The Cambridge Handbook of the Law of Algorithms*, Cambridge University Press, 2021, 616.
[77] Benjamin S, 'The First Amendment and Algorithms', 621.
[78] Bulka T, 'Algorithms and Misinformation: The Constitutional Implications of Regulating Microtargeting' 1112.
[79] Bulka T, 'Algorithms and Misinformation: The Constitutional Implications of Regulating Microtargeting' 1112.
[80] Bulka T, 'Algorithms and Misinformation: The Constitutional Implications of Regulating Microtargeting' 1112.
[81] Zarouali B, Dobber T, and Schreuder J, 'Personality and susceptibility to political microtargeting: A comparison between a machine-learning and self-report approach' 151 C*omputers in Human Behavior*, 2023, 1080.

term "psychographics-based targeting," as used by some scholars to refer to OPM,[82] is fitting.

Secondly, OPM distinguishes itself from PM by using algorithms to create personalised stories, feeds (e.g. personalised “For You” pages) and advertisements for users based on this information.[83] By programming these algorithms, these platforms can automatically select posts, links, and stories deemed appealing to specific users, and will therefore be prioritised at the top of users' search engine results and social media feeds.

Thirdly, OPM, unlike PM, is not limited to political adverts but instead includes all forms of political communication, such as tweets, Facebook posts, and Facebook ads.[84] Essentially, OPM is practised, intentionally or unintentionally, by citizens, political figures, and political campaigns alike. This is because it is disseminated by algorithms whose main purpose is to keep you interested and to do so, must present you with information that you are interested in,[85] which according to research, is information that aligns with your beliefs.[86] Therefore, referring to OPM merely as "political behavioural advertising," as some scholars do,[87] would be inaccurate, as OPM is more than just a marketing technique that tracks online behaviour to provide individually tailored political advertisements.

Nevertheless, it is necessary to discuss how OPM works as a marketing tool. OPM works in two distinct advertising mechanisms: Attribute-based Audiences technology (ABA) and Personally Identifying Information Audiences technology (PII).

2.2.1 Attribute Based Audiences

The first category of targeting tools, known as ABA, gives political campaigns the ability to choose a specific audience for an ad or campaign.[88] It operates by exploiting data that

[82] Zarouali B, Dobber T, De Pauw G, and de Vreese C, ‘Using a Personality-Profiling Algorithm to Investigate Political Microtargeting: Assessing the Persuasion Effects of Personality-Tailored Ads on Social Media,’ 49 *Communication Research* 8, 2022, 1079.
[83] Nott L, ‘Political Advertising on Social Media Platforms’ 45 *American Bar Association Journal* 3, 2020, 7.
[84] Bulka T, ‘Algorithms and Misinformation: The Constitutional Implications of Regulating Microtargeting' 1112.
[85] Benjamin S, ‘The First Amendment and Algorithms’, 623.
[86] Flaxman S, Goel S, and Rao J, ‘Filter Bubbles, Echo Chambers, and Online News Consumption,’ 312.
[87] Frederik J, Zuiderveen B, Möller J, Kruikemeier S, Fathaigh R, Irion K, Dobber T, Bodo B, and Vreese C, 'Online Political Microtargeting: Promises and Threats for Democracy,' 84.
[88] Casagran C and Vermeulen M, "Reflections on the murky legal practices of political micro-targeting from a GDPR perspective’ 11 *International Data Privacy Law* 4, 2021, 349.

social media platforms have previously collected and analysed about users. For instance, on Facebook, advertisers can pick from a variety of attributes such as geographical location, interests, connections, demographics, and behaviour.[89] It is crucial to highlight that in this form of advertising, the ad platform serves as the only data controller, and in principle, political campaigns do not have direct access to an individual's personal data.

2.2.2 Personally Identifying Information Audiences

The second category of targeting tools, which deals with ad delivery, is PII Audiences.[90] This tool is known by different names across platforms, for example, Custom Audiences on Facebook,[91] Tailored Audiences on Twitter,[92] and Customer Match Audiences on Google.[93] It provides political actors with the means to target their current contacts on the platform through a wide range of methods. The data that is mostly uploaded - though it varies from platform to platform - includes phone numbers, mobile advertiser IDs, and email addresses already in possession by the political actor. This data is then used to find the social media profiles linked to that data.

Some data sets are enough as stand-alone defining features for creating custom audiences, particularly on platforms like Facebook, where having an email address, phone number, mobile advertiser ID, or Facebook page user ID is sufficient.[94] Nevertheless, the amount of data that may be uploaded is unlimited, allowing political actors to introduce vast amounts of personal data theoretically. This data can be obtained through various methods, for example, from political party membership/donor registers.[95] Once the data is uploaded, the social media platform creates an audience corresponding to specified attributes. This process is facilitated by an algorithm which connects the initial personally

[89] 'How to use Facebook custom audiences' <https://support.google.com/adspolicy/answer/6299717?hl=en> on 4 January 2024.
[90] Venkatadri G, Andreou A, Liu Y, Mislove A, Gummadi P, Loiseau P, and Goga O, 'Privacy risks with Facebook's PII-based targeting: Auditing a data broker's advertising interface' *IEEE Symposium on Security and Privacy,* 2018, 91.
[91] 'How to use Facebook custom audiences' <https://www.facebook.com/business/help/744354708981227> on 4 January 2024.
[92] 'Tailored audiences' <https://business.twitter.com/en/help/campaign-setup/campaign-targeting/custom-audiences.html> on 4 January 2024.
[93] 'Google customer match help' <https://support.google.com/adspolicy/answer/6299717?hl=en> on 4 January 2024.
[94] 'How to use Facebook custom audiences' <https://www.facebook.com/business/help/744354708981227> on 4 January 2024.
[95] According to reports, a considerable percentage of data about voters acquired in both the 2013 and 2017 general elections was obtained from grassroots agents. See, Mutung'u, G, 'The Influence Industry Data and Digital Election Campaigning in Kenya,' 16.

identifiable information with individuals who have similar traits.[96]

Though most of these personal data categories may not explicitly disclose political affiliations, as indicated in the case of PM, they can still indirectly suggest a person's political inclinations. This is especially true when analysing this data collectively, as it enables the formation of a persona from which one's political opinions can be inferred.[97]

Additionally, when it comes to personalisation and customisation, certain social media platforms, such as Facebook, provide a unique feedback loop to advertisers, including political actors to enhance their ads and audiences. This means that online ads and social media content can dynamically adapt based on user interactions, allowing real-time adjustments to targeting strategies.[98] This process, which would be unachievable through traditional campaigning methods, enables them to discard users who are less likely to engage with the campaign.

Following from this, it is easy to see some of the appeals that OPM has in a democracy.

2.3 Benefits of OPM

When used in marketing, OPM enables campaigns and organisations to deliver targeted and substantive messages to citizens.[99] This approach ensures that citizens receive information that focuses on specific issues and policy goals rather than generic and irrelevant information that individuals may not find engaging or relevant to their concerns. This is significant for two reasons: Firstly, campaigns, especially those with limited resources such as upstart campaigns and grassroots movements, can optimise their efficiency, saving valuable time and resources.[100] Secondly, by utilising algorithms that prioritise policy goals aligned with citizens' interests, OPM not only reaches individuals who might typically overlook traditional media but also ignites their interest in politics with tailored messages. This in turn, contributes to heightened political awareness and

[96] Casagran C and Vermeulen M, "Reflections on the murky legal practices of political micro-targeting from a GDPR perspective,' 350.
[97] Casagran C and Vermeulen M, "Reflections on the murky legal practices of political micro-targeting from a GDPR perspective,' 351.
[98] Pariser, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think,* 62.
[99] Frederik J, Zuiderveen B, Möller J, Kruikemeier S, Fathaigh R, Irion K, Dobber T, Bodo B, and Vreese C, 'Online Political Microtargeting: Promises and Threats for Democracy,' 84.
[100] Frederik J, Zuiderveen B, Möller J, Kruikemeier S, Fathaigh R, Irion K, Dobber T, Bodo B, and Vreese C, 'Online Political Microtargeting: Promises and Threats for Democracy,' 88.

may even result in increased electoral turnout.[101]

Moreover, the online nature of OPM circumvents certain challenges associated with traditional media. This is particularly evident in democracies such as Kenya, where there have been instances of restricted press freedom. For example, during the 2017 elections, the government shut down traditional media outlets thus affecting television broadcasts. However, online activities of traditional media houses remained generally unaffected, allowing them to continue posting content despite the restrictions.[102]

It therefore comes as no surprise that the use of social media in the political sphere has consistently grown. Even though increased political engagement is advantageous for democracies, it must be recognised that not all applications of OPM are conducive to a peaceful democracy.

2.4 Downsides of OPM

The reason why OPM poses a greater threat to democracy, compared to traditional modes of political campaigning, is its use of filter bubbles and fake news.

2.4.1 Filter bubbles

As mentioned previously, OPM utilises much more detailed data profiles compared to other forms of political targeting. This allows social media platforms to use personalised content selection algorithms to customise and present content based on an individual's preferences and past behaviours.[103] This, in turn, creates a bubble around individuals, exposing them only to information that aligns with their beliefs and interests. It is this bubble that Parisier refers to as a "filter bubble."[104]

Filter bubbles are problematic as individuals not only find themselves confined to content that resonates with their established beliefs but are often unaware of this confinement. [105]

---

[101] Holt K, Shehata A, Strömbäck J, and Ljungberg E, 'Age and the effects of news media attention and social media use on political interest and participation: Do social media function as leveller?' 1 *European journal of communication*, 1, 2013, 27.

[102] Tweets by Business Daily and Nation Africa (also known as Daily Nation) <https://twitter.com/BD_Africa/status/960105657847263232> on January 4, 2024. <https://twitter.com/NationAfrica/status/959670285325680640> on January 4, 2024.

[103] Pariser, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think,* 105.

[104] Pariser, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think,* 105.

[105] Pariser, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think,* 134.

This lack of awareness is a concern in a democratic context for several reasons. Firstly, limited exposure reduces the diversity of perspectives people encounter, making it challenging for them to make well-informed and balanced decisions.[106] Secondly, the absence of diverse views contributes to societal polarization by reinforcing pre-existing beliefs and fostering an "us versus them" mentality. This polarization can lead to increased political and social division, creating difficulties for different groups to find common ground and engage in constructive dialogue.[107] Lastly, filter bubbles can give rise to echo chambers, where like-minded individuals reinforce each other's opinions, leading to a lack of critical thinking and fostering groupthink. Such a closed-minded environment can stifle innovation and hinder society's ability to adapt to changing circumstances.[108]

2.4.2 Fake news

The challenges posed by filter bubbles are exacerbated when the information within these bubbles is fake news. Fake news refers to both disinformation and misinformation.[109] Disinformation involves intentionally spreading false and misleading content on social media with the intent to deceive or manipulate users into believing it is true.[110] Misinformation, on the other hand, refers to the spread of inaccurate or false information without a deliberate intent to deceive. It occurs when individuals or sources unknowingly pass along information that is incorrect.[111]

This term gained prominence after the 2016 U.S. presidential elections, [112] where Russia strategically harnessed OPM to circulate fake news and influence the election's outcome.[113] This was achieved through recognising that algorithms employ OPM automatically, amplifying any news given sufficient user interaction rather than credibility. Realising this, Russia employed bots to propagate content. These bots played a key role by disseminating fake news and engaging with related posts to enhance

[106] Bozdag E and Van Den Hoven J, 'Breaking the filter bubble: democracy and design' 17 *Ethics and information technology* 1, 2015, 252.
[107] Bozdag E and Van Den Hoven J, 'Breaking the filter bubble: democracy and design,' 253.
[108] Bozdag E and Van Den Hoven J, 'Breaking the filter bubble: democracy and design,' 254.
[109] Kirdemir B, 'Exploring Turkey's Disinformation Ecosystem' *Centre for Economics and Foreign Policy Studies,* 2020, 4 - https://www.jstor.org/stable/resrep26087 on 7 January 2024.
[110] Merriam Webster Dictionary, 4 ed.
[111] Merriam Webster Dictionary, 4 ed.
[112] Allcott H and Gentzkow M, 'Social Media and Fake News in the 2016 Election' 213.
[113] Khan C, 'Despite report findings, almost half of Americans think Trump colluded with Russia' Reuters, March 27 2019
https://www.reuters.com/article/idUSKCN1R72SJ/ on 8 January 2024.

visibility. Once this content received the initial boost, actual users and citizens interacted with it, allowing it to be seen by even more users.[114] This happened because fake news often elicits extreme reactions, prompting people to engage with the post through likes, comments, and shares.[115] In a strategic move, Russian agents then combined this fake news campaign with the ABA marketing feature of OPM, effectively reaching an extensive audience of 126 million Facebook users.[116]

The fundamental issue with fake news, and perhaps even the reason misinformation exists, is the belief people place in it, which fuels its dissemination. This belief stems from the nature of human cognition.[117] Cognition is the process by which individual(s) process information. According to numerous studies, and as alluded to in the Russia case, the spread of false information is influenced by emotions, psychological factors, cognitive biases, preexisting beliefs, and mental shortcuts.[118] Consequently, the most effective cases of the spread of mis- and disinformation thrive on disseminating adverse and potentially harmful information that evokes fear, surprise and disgust, or targets biases, cognitive dependencies and conformity. These factors not only shape people's beliefs but also influence their receptiveness to interpersonal communication and external influence. Thus, fake news should be viewed "not as low-quality information that spreads because of the inefficiency of online communication, but as high-quality information that spreads because of its efficiency. The difference is that 'quality' is not equated to truthfulness but psychological appeal".[119]

Additionally, the evolution of fake news into what RAND Corporation labels as a tool of "hostile social manipulation" intensifies its effects.[120] RAND Corporation categorises fake news this way due to its intentional and systematic creation and dissemination of information with the aim of achieving detrimental social, economic, and political consequences by influencing beliefs, behaviours, and attitudes. This manipulation of fake

[114] Wakabayashi D, 'Russian Influence Reached 126 Million Through Facebook Alone', The New York Times, October 30 2017 <https://perma.cc/5X63-VM62> on 9 January 2024.
[115] Allcott H and Gentzkow M, 'Social Media and Fake News in the 2016 Election' 213.
[116] Wakabayashi D, 'Russian Influence Reached 126 Million Through Facebook Alone', The New York Times, October. 30, 2017 <https://perma.cc/5X63-VM62> on 9 January 2024.
[117] Acerbi A, 'Cognitive Attraction and Online Misinformation' 5 *Palgrave Communications* 1, 2019, 7.
[118] Acerbi A, 'Cognitive Attraction and Online Misinformation' 11.
[119] Acerbi A, 'Cognitive Attraction and Online Misinformation,' 15.
[120] Rand corporation, *Hostile Social Manipulation: Present Realities and Emerging Trends*, 2019, 33.

news leverages cyber mediums, employing various techniques such as disinformation, propaganda (including the use of botnets), trolling, the generation of fake content, and imposter accounts — all of which rely on OPM to gain traction.[121]

2.5 Kenya's Experience with OPM

Contrary to the belief by some scholars that OPM is exclusively a concern in Western countries,[122] this section highlights its relevance in Kenyan politics by using both the 2017 and 2022 elections as case studies.

In the 2017 elections, Harris Media LLC effectively employed Google ad services and leveraged ABA to disseminate two highly provocative videos: "The Real Raila" and "Uhuru for Us." These videos aimed to exploit Kenya's tumultuous history by instilling fear in voters. Specifically, "The Real Raila" campaign claimed that the opposition candidate's presidency would lead to the "elimination of whole tribes."[123]

Then, in 2022, in the lead-up to voting day, a barrage of false claims further muddied social media. For instance, OPM was used to circulate unsubstantiated reports suggesting wild animals had escaped and were loose. In other regions, baseless claims of military deployment were spread, all in a bid to reduce voter turnout.[124] Additionally, Raila Odinga's Azimio la Umoja-One Kenya Coalition camp shared a video that manipulated subtitles to distort the image of William Ruto, leader of the Kenya Kwanza Coalition. The manipulated subtitles falsely indicated that Ruto was threatening citizens who were not Kalenjins in his local dialect. However, Ruto was actually guaranteeing communities outside the Kalenjin tribe of their safety in the region and encouraging them to continue with their daily lives.[125] This circulation of fake news could amount to hostile social manipulation because political parties used all means at their disposal to circulate the fake news — from paying social media platforms and influencers, to employing bots that created numerous accounts to popularise content and allowing algorithms to further spread

---

[121] Rand corporation, *Hostile Social Manipulation: Present Realities and Emerging Trends*, 2019, 219.
[122] Mude H, 'Political Micro-Targeting in Kenya: An Analysis of the Legality of Data Driven Campaign Strategies under the Data Protection Act' 8.
[123] Dommett K, 'Data-driven political campaigns in practice: understanding and regulating diverse data-driven campaigns,' 13.
[124] Madung O, 'From Dance App to Political Mercenary: How disinformation on TikTok gaslights political tensions in Kenya' *Mozilla Report*, 2022, 14 - https://foundation.mozilla.org/en/campaigns/kenya-tiktok/ on 9 January 2024.
[125] Madung O, 'From Dance App to Political Mercenary: How disinformation on TikTok gaslights political tensions in Kenya' *Mozilla Report*, 2022, 14 - https://foundation.mozilla.org/en/campaigns/kenya-tiktok/ on 9 January 2024.

it.

The surge in false news becomes problematic during political campaigns, with 75% of Kenyan news consumers struggling to differentiate between genuine and fake news online, according to a Reuters Institute survey.[126] This susceptibility to fake news poses a grave threat to the democratic process in Kenya, because when voters fall prey to calculated disinformation campaigns or outright false claims, it erodes democracy. This is because democracy relies on a mutual understanding of objective facts,[127] and when this common ground is eroded, voting decisions may be called into question as they may not reflect the genuine will of the people.

For these reasons, it is crucial that regulations guard against these effects of OPM.

2.6 The Inadequacy of Present Regulation

In 2010, Kenya promulgated a constitution, which safeguards the right to free and fair elections under article 38.[128] However, with the emergence of OPM, this right is at stake, as illustrated in the previous section. Therefore, it is imperative to ensure that legislation regulates either OPM or its effects. Despite this need, Kenya currently lacks specific legislation governing OPM, and the aim of this part of the paper is to explore whether existing laws can be used to regulate the practice. The focus of this investigation will be on the Data Protection Act (given scholars often view OPM as a data-related issue) and the Computer Misuse and Cybercrimes Act (the primary legislation governing cyberspace).

2.6.1 The Inadequacy of Kenya's Data Protection Act

The Data Protection Act (DPA), passed in 2019, primarily regulates the processing of personal data by providing that, in order to process personal information, a data controller or processor must obtain the consent of the data subject, which must be "unequivocal, free, specific and informed".[129]

---

[126] Olivia L, 'Disinformation was rife in Kenya's 2022 election', Africa at LSE, January 5 2023 https://blogs.lse.ac.uk/africaatlse/2023/01/05/disinformation-was-rife-in-kenyas-2022-election/ on 7 January 2024.

[127] Sugow A, 'The Right to be Wrong: Examining the (Im)possibilities of Regulating Fake News while Preserving the Freedom of Expression in Kenya', 4 *Strathmore Law Review* 1, 2019, 7.

[128] Article 52, *Constitution of Kenya* (2010).

[129] Section 32, *Data Protection Act* (2019).

At the time of passing the DPA, regulators deemed it sufficient to regulate OPM they perceived OPM to be solely a tool that infringed on individual privacy.[130] Consequently, the act was designed to protect the privacy of users and protect against the marketing features of OPM. This position stemmed from the fact that during the 2017 elections, fake news was spread via political ads on social media platforms. For instance, Harris Media LLC relied on the PII audience feature to spread the two highly aggressive videos, mentioned previously, and the data uploaded to target individuals was done without their consent.[131] Then, even for smaller parties using the ABA feature, the data relied upon was not obtained with proper consent, as social media platforms rarely provided users with the opportunity to consent to their data being used for OPM.[132] Thus, scholars like Mude and regulators viewed OPM as a privacy issue. They contended that this act was adequate to regulate against the effects of OPM, since it mandated platforms and political parties to seek citizens' consent before using and processing their personal information.[133]

As a result, while the enactment of the DPA was a commendable step forward, it was put in place to only regulate the marketing features of OPM. However, even for these features, the act was insufficient in addressing the adverse effects of OPM as will be seen.

A. Shortcomings of Kenya's DPA in regulating PII audiences

First and foremost, the DPA faces limitations in effectively regulating OPM due to the vague and ambiguous nature of its provisions, particularly when applied to OPM practices. Designed as an omnibus law, the DPA aims to be applicable to a wide range of personal data usage scenarios in both private and public sectors.[134] However, this broad application results in the formulation of vague rules. For example, there is difficulty in identifying the data controller, despite the DPA's requirement that the data controller must obtain consent.[135] This challenge becomes especially pronounced in PII audience

[130] Mude H, 'Political Micro-Targeting in Kenya: An Analysis of the Legality of Data Driven Campaign Strategies under the Data Protection Act,' 12.
[131] Muthuri R, Karanja M, Monyango F and Karanja W, 'Investigating privacy implications of biometric voter registration In Kenya's 2017 election Process,' 32.
[132] Muthuri R, Karanja M, Monyango F and Karanja W, 'Investigating privacy implications of biometric voter registration In Kenya's 2017 election,' 17.
[133] Mude H, 'Political Micro-Targeting in Kenya: An Analysis of the Legality of Data Driven Campaign Strategies under the Data Protection Act' 21.
[134] Section 4 and 8, *Data Protection Act* (2019).
[135] Section 28, *Data Protection Act* (2019).

advertising. Should the platform where the data is uploaded be considered the data controller, given its possession and utilisation of the information to target users? Alternatively, are the data controllers the third parties collecting this data or orchestrating online political campaigns? Or could it be the political parties themselves, benefiting from the work of hired third parties? The lack of clarity in these instances complicates the enforcement of consent-related obligations under the DPA.

Furthermore, studies, such as the one conducted by Deloitte and reported by Business Insider, reveal that 60% of citizens willingly share data in exchange for personalised benefits and discounts.[136] Political campaigns in Kenya leverage this willingness by offering incentives like free services, products, or vouchers in exchange for consent to utilise personal data.[137] In doing so, these campaigns strategically circumvent the DPA, leaving the public vulnerable to the potential harms of OPM.

B. Shortcomings of Kenya's DPA in regulating ABA features

As previously discussed, platforms that engage in political microtargeting require user data, which can be either uploaded by third parties (PII audiences) or obtained directly by the platform (as in the case of ABA). When this data is obtained by the platform, data collection heavily relies on electronic tools such as 'Cookies,' 'Social Plugins,' and 'Tracking Pixels.'[138]

Before the implementation of the DPA, the acquisition of this data often occurred without explicit consent. The DPA sought to address this by requiring that explicit consent be provided before the collection of personal data.[139] However, what was unforeseen was the willingness of many individuals to grant consent to be microtargeted. By "many," this paper refers to the fact that, even with tools like incognito mode available, only a mere 1.13% of internet users take the initiative to manually delete their cookies or browse incognito.[140] Additionally, a survey conducted by Deloitte found that 91% of

[136] Deloitte, *Cookies bench study,* 2020, 29-40.
[137] Rutenberg I and Sugow A, 'Regulation of the Social Media in Electoral Democracies: A Case of Kenya,' 31.
[138] https://ico.org.uk/for-the-public/be-data-aware/social-media-privacy-settings/microtargeting/ on 5 January 2024.
[139] Section 32, *Data Protection Act* (2019).
[140] Papadopoulos P, Markatos E, Kourtellis N, 'Cookie Synchronisation: Everything You Always Wanted to Know But Were Afraid to Ask,' *Research Gate*, 13 May 2018, 14

individuals—and 97% of young people—consent to legal terms and service conditions without actually reading them, thus allowing for OPM.[141] This low rate of manual intervention allows platforms to persistently track users' online activities, thereby facilitating OPM. Several factors contribute to this situation.

For starters, a considerable number of users actively seek and want to receive information that aligns solely with their beliefs,[142] essentially embracing the concept of filter bubbles. Moreover, about a quarter of users (24%) mistakenly believe that rejecting cookies will result in redirection or exclusion from a website.[143] While this is not accurate, the consequence of non-consent is the loss of access to certain parts of platforms,[144] so their fear can be said to be grounded in some truth.

Additionally, some users consent due to the complexity of the terms and conditions presented by social media platforms. The DPA not only requires consent but also mandates that this consent must be specific, [145] leading platforms to create extensive terms and conditions to cover all aspects and reduce their liability. However, the drawback is that these lengthy terms become impractical for users to read comprehensively, with a study done finding that the average person would need to allocate 250 hours annually to properly go through all the digital contracts they accept when using online services.[146] While this study was based on Americans and pertains to all online services, not just social media platforms, it still highlights the impracticality of people reading terms and conditions.

https://dl.acm.org/doi/abs/10.1145/3308558.3313542#:~:text=Cookie%20Synchronization%20work%3F-,Cookie%20Synchronization%3A%20Everything%20You%20Always%20Wanted%20to,But%20Were%20Afraid%20to%20Ask&text=User%20data%20is%20the%20primary,to%20data%20markets%20and%20advertisers on 9 January 2024.

[141] Cakebread C, 'You're not alone, no one reads terms of service agreement', Business Insider, 15 November 2017 https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11?r=US&IR=T on 4 January 2024.

[142] Flaxman S, Goel S, and Rao J, 'Filter Bubbles, Echo Chambers, and Online News Consumption,' 307.

[143] Koebert J, 'Cookies Study: 40% of Americans Blindly Accept Internet Cookies, But Most Don't Know What They Do' 21 September 2023 https://allaboutcookies.org/internet-cookies-survey on 5 January 2024.

[144] Koebert J, 'Cookies Study: 40% of Americans Blindly Accept Internet Cookies, But Most Don't Know What They Do' 21 September 2023 https://allaboutcookies.org/internet-cookies-survey on 5 January 2024.

[145] Section 32, *Data Protection Act* (2019).

[146] Cohen J, 'It Would Take 17 Hours to Read the Terms & Conditions of the 13 Most Popular Apps' PC gamer Newsletter, 4 December 2020 https://www.pcmag.com/news/it-would-take-17-hours-to-read-the-terms-conditions-of-the-13-most-popular 5 January 2024.

Lastly, it's important to mention that, even if individuals choose not to consent to their data being taken and utilised, they can still be targeted as this information can be inferred. A study conducted by Korolova in 2011 demonstrated that advertisers, using ABA technology on Facebook, could accurately infer the sexual orientation of a non-friend, even when the user shared their status in a 'Friends Only' visibility mode.[147] Numerous similar experiments on Facebook have highlighted the platform's ability, through 'likes' and content uploaded by other users, to automatically and accurately predict sensitive personal attributes such as sexual orientation, ethnicity, religion, gender, and political views.[148]

Taken collectively, these factors illustrate that people consent to political microtargeting by platforms, rendering the DPA ineffective in mitigating the adverse effects of OPM.

2.6.2 The Problem of the Computer Misuse and Cybercrimes Act

Passed in 2018, this act was celebrated for being the first act governing the online space and the only one regulating fake news. Even so, this act proves insufficient in regulating against OPM and its effects.[149]

Presently, the act it concentrates solely on regulating individual users.[150] It lacks specific measures, such as take-down laws or procedures, to address the involvement of social media platforms. This creates an ironic situation where the posting of fake news is prohibited but, if done, social media platforms' and their algorithms are permitted to circulate and propagate the fake news.

This approach to regulation may not even be effective. A study conducted by USIU revealed that 47.7% of Kenyans use pseudonyms when accessing social media.[151] This indicates that law enforcement would face challenges in identifying users who create and

---

[147] Korolova A, 'Privacy Violations using Microtargeted Ads: A Case Study' 3 *Journal of Privacy and Confidentiality* 1, 2011, 35.
[148] Thomas K, Grier C and Nicol D, *'Unfriendly: Multi-party Privacy Risks in Social Networks'*, Springer Berlin Heidelberg, 21 May 2010, 237 https://link.springer.com/chapter/10.1007/978-3-642-14527-8_14 on 10 January 2024.
Kosinski M, Stillwell D and Graepe T, 'Private Traits and Attributes are Predictable from Digital Records of Human Behavior' 110 *Proceedings of the National Academy of Sciences of the United States of America* 15, 2013, 31.
[149] Section 22 and 23, *Computer Misuse and Cybercrimes Act* (2018).
[150] Section 3, *Computer Misuse and Cybercrimes Act* (2018).
[151] Wamuyu P, 'The Kenyan Social Media Landscape: Trends and Emerging Narratives' Research Anthology on Usage, Identity, and Impact of Social Media on Society and Culture,' 840.

disseminate fake news. Moreover, considering that fake news is often posted and spread by bots,[152] tracing the individuals behind these bots becomes even more difficult.[153] Consequently, the regulation of fake news, OPM, and its associated adverse effects remains largely unaddressed.

2.7 Conclusion

The chapter has provided an in-depth analysis of what OPM is, highlighting its potential benefits within a democracy. Nevertheless, it has equally showcased the inherent dangers associated with OPM within a democratic context. Moreover, the chapter has demonstrated the limitations of existing legislation in effectively addressing and mitigating these inherent dangers. In light of this, the subsequent chapter will focus on assessing the different approaches countries have taken to regulate OPM, dissecting their distinct advantages and disadvantages.

[152] Rutenberg I and Sugow A, 'Regulation of the Social Media in Electoral Democracies: A Case of Kenya,' *School of Oriental and African Studies Law Journal*, 2020, 39.
[153] Rutenberg I and Sugow A, 'Regulation of the Social Media in Electoral Democracies: A Case of Kenya,' 39.

3.0 GLOBAL APPROACHES TO REGULATING OPM

3.1 Introduction

As demonstrated in Chapter 2, the shortcomings of current laws in Kenya in regulating OPM highlight the need for a deeper examination of regulatory approaches to counter its adverse effects. However, as has been shown in the previous chapter, merely regulating users is insufficient; there is a need to regulate platforms. This is due to the fact that the algorithms employed by platforms facilitate the existence of filter bubbles and allow for misinformation and disinformation to thrive. Nevertheless, controlling platforms to mitigate such content is a complex task. Thus, this chapter delves into various global regulatory approaches adopted by different jurisdictions to tackle the challenges posed by OPM.

These regulatory strategies are categorised into three principal approaches: The Banning Approach, Information Control Approach and Neutral Approach. The proceeding sections of this chapter will scrutinise each approach, outlining its respective merits and demerits.

3.2 The Banning Approach

The first approach, termed the "banning approach," advocates for an outright prohibition of either political ads which are micro-targeted on social media platforms or on all ads on social media platforms. It is crucial to acknowledge that when countries adopt this regulatory approach for OPM, they are specifically focusing on the marketing features of OPM. Hence, they are overlooking the fact that micro-targeting extends beyond just paid ads, encompassing everything presented on platforms tailored to individual interests.

The logic behind countries choosing this form of regulation becomes evident when considering the aftermath of the 2016 presidential elections in the USA. In that election, Russian agents exploited various features of OPM to influence outcomes and disseminate misinformation. While multiple OPM features were utilised, the focus of the criticism was the use of Facebook ad features.[154] Consequently, many countries opted for the banning approach to regulate OPM in response to such incidents.

[154] Khan C, 'Despite report findings, almost half of Americans think Trump colluded with Russia:' Reuters, March 27 2019
https://www.reuters.com/article/idUSKCN1R72SJ/ on 8 January 2024.

For example, in France, social media platforms are prohibited from engaging in any commercial advertising for the use or for the purpose of election propaganda during the six months leading up to an election.[155] Moreover, in a bid to regulate all types of indirect political advertising that might take place during that period - where ad campaigns may not overtly endorse a specific party or candidate but convey messages aligned with their agenda[156] - the law stipulates that in the three months preceding elections, online platforms must furnish users with information regarding the financial backers of the "promotion of content related to a debate of general interest."[157]

3.2.1 Advantages of Banning Approach

This approach offers several advantages, foremost among them being the fact that if widely implemented, a ban on microtargeting could compel platforms to discontinue the use of algorithms entirely for content generation, or at the very least, necessitate adjustments in algorithmic inputs thus preventing the formation of filter bubbles.[158] Furthermore, this approach serves as an effective deterrent against both political parties spreading false information through paid advertisements[159] and, to a certain extent, guards against external interference from other countries, like was witnessed in the 2016 USA presidential elections.[160]

Moreover, the banning approach presents a notable advantage in terms of implementation cost. Since it places a negative duty on social media platforms - essentially requiring them to refrain from specific activities rather than taking on new obligations - the associated costs are comparatively low.[161] Nonetheless, some may argue that this approach could be considered expensive for countries due to the potential loss of revenue resulting from the absence of political advertisements on platforms.[162]

---

[155] Article L. 52-1, *Code electoral* (France).
[156] Dobber T, Fathaigh R and Borgesius F, 'The regulation of online political micro-targeting in Europe' 45.
[157] Article L. 163-1, *Code electoral* (France).
[158] Bulka T, 'Algorithms and Misinformation: The Constitutional Implications of Regulating Microtargeting'14.
[159] Couzigou I, 'The French Legislation Against Digital Information Manipulation in Electoral Campaigns: A Scope Limited by Freedom of Expression' 20 *Election Law Journal: Rules, Politics and Policy 1,* 2021, 112.
[160] Couzigou I, 'The French Legislation Against Digital Information Manipulation in Electoral Campaigns: A Scope Limited by Freedom of Expression,' 109.
[161] Couzigou I, 'The French Legislation Against Digital Information Manipulation in Electoral Campaigns: A Scope Limited by Freedom of Expression' 101.
[162] Couzigou I, 'The French Legislation Against Digital Information Manipulation in Electoral Campaigns: A Scope Limited by Freedom of Expression,' 102.

In essence, while these benefits have prompted countries to adopt this approach, it still has certain drawbacks that may negate these benefits.

3.2.2 Disadvantages in Implementing a Ban

A ban on OPM is not a comprehensive solution to the issues associated with this practice. While regulating political advertisements is a step, it fails to address broader problems such as the creation of filter bubbles and the perpetuation of confirmation bias. This is because, even without political ads, platforms can still algorithmically tailor content to users, fostering echo chambers and limiting exposure to diverse perspectives.[163]

Moreover, focusing solely on false and misleading advertisements overlooks the broader scope of disinformation. It is not just ads that can spread fake news; news stories and individual posts not be classified as advertisements also contribute to the spread fake news.[164] Consequently, a ban narrowly focused on deceptive ads still permits the dissemination of fake news.[165] In this scenario, while there might be a marginal reduction in the scale of false news, the fundamental problem persists without resolution.

On top of this, a ban on the advertising features of OPM results in a loss of numerous benefits of OPM. This has significant implications, particularly for small upstart and grassroots campaigns, as it compels them to allocate more of their limited resources to less effective forms of communication.[166]

Such a ban also serves to protect incumbents, wealthy individuals, and celebrity candidates who already possess name recognition, media access, and a robust fundraising base.[167] In contrast, challengers often lack these assets at the start of their campaigns and may not be widely known.[168] However, microtargeting makes it easier for challengers to become competitive relatively cheaply. Consequently, a prohibition on ad targeting

[163] Rutenberg I and Sugow A, 'Regulation of the Social Media in Electoral Democracies: A Case of Kenya,' *School of Oriental and African Studies Law Journal*, 2020, 39.
[164] Bulka T, 'Algorithms and Misinformation: The Constitutional Implications of Regulating Microtargeting,' 1111.
[165] Bulka T, 'Algorithms and Misinformation: The Constitutional Implications of Regulating Microtargeting,' 1116.
[166] Institute for Free Speech, *The Truth About "Microtargeting" and Political Speech: Why a Ban Is a Bad Idea,* 2021, 3.
[167] Institute for Free Speech, *The Truth About "Microtargeting" and Political Speech: Why a Ban Is a Bad Idea,* 2021, 3.
[168] Institute for Free Speech, *The Truth About "Microtargeting" and Political Speech: Why a Ban Is a Bad Idea,* 2021, 3.

would disproportionately disadvantage challengers while providing advantages to incumbents, wealthy individuals, and celebrity candidates.

In summary, while this regulatory approach brings certain advantages, it also introduces complexities and potential unintended consequences that need careful consideration.

3.3 Neutral Approach

In the neutral approach to regulation, the government seeks a middle ground, aiming to balance the protection of freedom of expression with limited regulation. This approach avoids restricting the marketplace of ideas, acknowledging that legislation holding social media platforms strictly accountable might hinder the free flow of information.[169] Instead, the regulation requires social media platforms to take reasonable measures to ensure accessibility, due diligence, privacy, and transparency. By meeting these criteria, platforms are accorded safe harbour provisions.[170] The underlying rationale is that social media platforms will engage in self-regulation out of economic self-interest to safeguard their valuable brands.[171] This approach relies on the assumption that the economic incentive for platforms to protect their brand reputation will naturally lead to responsible behaviour, fostering a regulatory environment that encourages self-governance while preserving freedom of expression.[172]

This approach is reflective of the USA, which aligns with the principles of a "democratic capitalist political-economic system".[173] The USA, following this approach, provides safe harbour provisions for platforms under Section 230 Communications Decency Act. This provision shields intermediaries (social media platforms) from legal liability for user-posted content.[174] However, compliance is contingent upon the adherence to the

[169] Citron D and Benjamin W, 'The internet will not break: Denying bad Samaritans section 230 immunity' 1 *Fordham Law Review* 86, 2017,401.
[170] A safe harbour is a legal provision to sidestep or eliminate legal or regulatory liability in certain situations, provided that certain conditions are met. See, Hayes A, ' What Is a Safe Harbor? Types, and How They Are Used' Investopedia, November 21 2020 https://www.investopedia.com/terms/s/safeharbor.asp on 5 January 2024.
[171] Citron D, and Benjamin W, 'The internet will not break: Denying bad Samaritans section. 230 immunity,' 409.
[172] Citron D, and Benjamin W, 'The internet will not break: Denying bad Samaritans section. 230 immunity' 405.
[173] Bartlett A, 'Different Strokes: Political and Economic Systems Around the Globe' Lumen learning, February 12 2021 https://courses.lumenlearning.com/suny-internationalbusiness/chapter/reading-capitalism-in-the-us/#:~:text=Democratic%20capitalism%2C%20also%20known%20as,predominantly%20on%20a%20democratic%20polity on 7 January 2024.
[174] Section 230, *Communications Decency Act* (The United States).

Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021. Rule 3(1)(m) specifically mandates that intermediaries take reasonable measures to ensure service accessibility, coupled with expectations of due diligence, privacy, and transparency.[175]

The rationale for this approach is rooted in the recognition that it would be practically impossible for platforms to monitor and control all content on social media. In the USA, this reasoning emerged from the case *Stratton Oakmont, Inc. v Prodigy Services Co.* In this landmark case, Prodigy, an early online service provider, implemented software to filter profanity with the intention of attracting families to its services. However, when a user posted defamatory comments about a securities firm on a financial bulletin board, Prodigy found itself facing a lawsuit which argued that it was strictly liable as the publisher of the defamation, just like other conventional publishers would be.[176]

The court's decision, which held Prodigy liable despite its efforts to filter objectionable content, drew the attention of lawmakers. The turning point was when Prodigy's immunity as a distributor was revoked and it assumed liability as a publisher due to its attempt to remove objectionable material.[177] In response, Congress acted to grant immunity for screening activities. The concern was that holding online service providers accountable for imperfect screening might discourage any screening at all, as providers could evade liability by assuming a passive conduit role.[178] Lawmakers believed that the responsibility of monitoring objectionable content online surpassed the capabilities of public regulatory agencies, thus self-regulation was necessary.

3.3.1 Disadvantages of the Neutral Approach

The issue with the immunity provided under this approach is its perceived lack of limitations, leading to unintended consequences. In the USA, platforms have continued to enjoy immunity, even when involved in actions such as republishing content with knowledge of potential law violations, encouraging users to post illegal content, adjusting their platform policies and design to facilitate illegal activity, or participating in the sale

[175] Rule 3(1)(m), *Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules*, 2021.
[176] *Stratton Oakmont, Inc. v Prodigy Services Co.* (1995), New York Supreme Court.
[177] *Stratton Oakmont, Inc. v Prodigy Services Co.* (1995), New York Supreme Court.
[178] Congressional Record Vol.141, 4 August 1995, 30.

of dangerous products.[179] Further, numerous legal decisions have consistently extended this broad immunity, with instances of denial or restriction remaining relatively few.[180] Yet, proponents of this approach argue that, despite these negative outcomes, the alternative of imposing stringent regulations on platforms to control speech is worse.

3.3.2 Advantages of the Neutral Approach

Proponents of this approach argue that the primary goal of this approach is not to protect platforms but to preserve freedom of speech.[181] To them, in a world without safe harbour protections, platforms facing potential liability for content on their sites would likely become more risk-averse, leading to the removal of a significant amount of content to avoid the possibility of facing a lawsuit. For example, the #MeToo movement might have unfolded very differently in a world where platforms removed any posts that even remotely looked defamatory.[182]

Another reason why the neutral approach may be preferred is the challenges posed by alternative regulatory strategies. The other approaches necessitate extensive legislation and specificity, a daunting task given that social media platforms operate on the internet, which has a dual nature: a global commons and a privately owned and operated space.[183] Practically, it is also challenging to enact laws that can keep pace with the rapid developments characteristic of these platforms.[184] Furthermore, in Africa, the complexity is heightened by the fact that these platforms are often owned and operated by foreign entities.[185] Therefore, embracing broad and vague requirements, as in the neutral approach, could be considered beneficial.

---

[179] Citron D, *'Hate crimes in cyberspace'*, Harvard University Press, 2014, 16.
[180] Citron D, *'Hate crimes in cyberspace'*, Harvard University Press, 2014, 16.
[181] Witte M, 'Four questions: Evelyn Douek, on what Section 230 is and why it is misunderstood', Stanford News, 7 October 2022 https://news.stanford.edu/2022/10/07/four-questions-evelyn-douek-section-230-misunderstood/ on 8 January 2024.
[182] Witte M, 'Four questions: Evelyn Douek, on what Section 230 is and why it is misunderstood', Stanford News, 7 October 2022 https://news.stanford.edu/2022/10/07/four-questions-evelyn-douek-section-230-misunderstood/ on 8 January 2024.
[183] Rutenberg I and Sugow A, 'Regulation of the Social Media in Electoral Democracies: A Case of Kenya,' 28.
[184] Rutenberg I and Sugow A, 'Regulation of the Social Media in Electoral Democracies: A Case of Kenya,' 30.
[185] Rutenberg I and Sugow A, 'Regulation of the Social Media in Electoral Democracies: A Case of Kenya,' 30.

To sum up, despite the drawbacks associated with this approach, it's understandable why countries would choose to adopt it.

3.4 Information Control Approach

This regulatory approach entails imposing stringent regulations on platforms, compelling them to actively address the harmful effects of OPM. The best of this approach is the NetzDG law in Germany, colloquially known as a "hate speech law." [186] Enacted in 2018, this law has gained attention for being the most ambitious effort by a state to hold social media platforms accountable for combating online speech[187] Despite its planned expiration in February 2024, when the EU Digital Services Act takes effect,[188] NetzDG remains a benchmark for this approach as it has influenced legislation in 25 countries.[189]

3.4.1 Advantages of the Information Control Approach

To comprehend the advantages of the Information Control Approach, it is essential to examine key aspects of NetzDG that showcase its effectiveness in addressing mis- and disinformation. One crucial element is the requirement for platforms to establish a mechanism for users to report illegal content.[190] Under the NetzDG, upon receiving a complaint, platforms must investigate and promptly remove "manifestly unlawful" content within 24 hours, while other illegal content must be taken down within 7 days.[191] Failure to comply may result in fines of up to €50 million.[192] This provision incentivises platforms not only to take down fake news upon reporting but also to proactively reprogram algorithms to identify and remove such content.

Another notable feature of this approach is that, out of all the other approaches, it is the only approach that tries to mitigate the issue of filter bubbles. The Digital Services Act, modelled after the NetzDG, regulates the information platforms can use in targeted advertising. It specifically restricts the use of personal attributes like sexual orientation,

[186] Transatlantic Working Group, *An Analysis of Germany's NetzDG Law,* 2019, 3.
[187] Transatlantic Working Group, *An Analysis of Germany's NetzDG Law,* 2019, 10.
[188] Griffin R 'New School Speech Regulation (NSSR) and Online Hate Speech: A Case Study of Germany's NetzDG', Unpublished Thesis, Hertie School, Berlin, 2021, 50.
[189] Griffin R 'New School Speech Regulation (NSSR) and Online Hate Speech: A Case Study of Germany's NetzDG', Unpublished Thesis, Hertie School, Berlin, 2021, 53.
[190] Sections 2-4. *Network Enforcement Act* (Germany).
[191] Sections 2-4. *Network Enforcement Act* (Germany).
[192] Sections 2-4. *Network Enforcement Act* (Germany).

religion, ethnicity, or political beliefs when engaging in OPM.[193] This means that, using this method, countries can effectively guard against platforms collecting sensitive data that could serve as a proxy for a person's political views. However, despite widespread adoption, the Information Control Approach is not without its disadvantages

3.4.2 Disadvantages of the Information Control Approach

A major concern of this approach is the potential for bias towards over-removal, infringing on the freedom of expression.[194] Critics argue that social media platforms lack the expertise and time to thoroughly assess each complaint, given that legal evaluations often demand extensive knowledge of the local language and jurisprudence, coupled with a complex case-by-case investigation and analysis. Consequently, due to the costs involved, as well as the tight deadlines and hefty fines imposed by regulations like NetzDG, platforms may opt to comply with most complaints, irrespective of their merits, leading to over-removal.[195]

Another point of contention is the privatisation of enforcement, where platforms, rather than courts or democratically legitimated institutions, assess the legality of content.[196] However, the counterargument gains credence when considering that due to the scale and technical operations of online platforms, it is impractical for state institutions to handle first-instance moderation decisions.[197]

Furthermore, scholars argue that if states were to take over supervision, detailed state oversight of online communications would raise significant free speech concerns.[198] However, it is not problematic for platforms to undertake this role, as they already exert extensive control over users' information environments for commercial purposes.

---

[193] Tworek H and Leerssen P, 'An Analysis of Germany's NetzDG Law,' *Transatlantic Working Group Working Paper* accessed 12 July 2019 <https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf> on 9 January 2024.

[194] Griffin R, *New School Speech Regulation (NSSR) and Online Hate Speech: A Case Study of Germany's NetzDG*, 2021, 47.

[195] Schulz W, 'Regulating intermediaries to protect privacy online–the case of the German NetzDG', *Personality and Data Protection Rights on the Internet*, 8 March 2021 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3216572 on 9 January 2024.

[196] Griffin R, *New School Speech Regulation (NSSR) and Online Hate Speech: A Case Study of Germany's NetzDG*, 2021, 50.

[197] Griffin R, *New School Speech Regulation (NSSR) and Online Hate Speech: A Case Study of Germany's NetzDG*, 2021, 50.

[198] Heldt A, 'Reading between the lines and the numbers: an analysis of the first NetzDG reports', 8 *Internet Policy Review* 2, 2019, 15.

Consequently, regulations incentivising interventions to address hate speech are not inherently objectionable. Moreover, leaving platforms' private opinion power unregulated is considered unlikely to serve media freedom or free speech, as they have been observed to arbitrarily censor minorities and political speech. Thus, this approach is preferable because it offers stronger procedural safeguards compared to standard contractual relationships with platforms, which typically provide no recourse against censorship.[199]

An additional critique of this approach questions its effectiveness due to challenges in implementation.[200] For instance, studies on content moderation and its impact on banned content reveals that only a fraction of hate speech and fake news is effectively addressed.[201] To explain why this is so, it is imperative to first start by explaining the workings of current content moderation practices. These practices rely on a combination of automated content recognition and user reporting, both of which prove unreliable as they exhibit high rates of false negatives (overlooking fake news and hate speech) and false positives (removing non-hateful content on the grounds it is fake news or vice versa).[202]

The issue of false negatives arises because much misinformation and disinformation go unreported, either due to being seen by sympathetic audiences or because platform affordances make reporting laborious.[203] Ironically, this reporting has instead been maliciously used against victims of discrimination.[204] On the other hand, is automated moderation which is evidently more efficient and less prone to deliberate misuse. However, it remains notoriously unreliable, particularly for complex, context-dependent categories like fake news and hate speech. Moreover, commercial moderation software, widely available, tends to disproportionately remove speech from marginalised groups,

[199] Griffin R, *New School Speech Regulation (NSSR) and Online Hate Speech: A Case Study of Germany's NetzDG*, 2021, 50.
[200] Critics include local digital rights organisations such as Netzpolitik, international groups such as Access Now, Article 19, and European Digital Rights (EDRi). One prominent German academic critic is Wolfgang Schulz, Director of the Hans Bredow Institute for Media Research. See,
Schulz W, 'Regulating intermediaries to protect privacy online–the case of the German NetzDG', *Personality and Data Protection Rights on the Internet*, 8 March 2021 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3216572 on 9 January 2024.
[201] Heldt A, 'Reading between the lines and the numbers: an analysis of the first NetzDG reports,'15.
[202] Zurth P, 'The German NetzDG as a role model or cautionary tale? Implications for the debate on social media liability' 4 *Fordham Intellectual Property Media & Entertainment. Law Journal*, 2020, 31.
[203] Heldt A, 'Reading between the lines and the numbers: an analysis of the first NetzDG reports,'19.
[204] Zurth P, 'The German NetzDG as a role model or cautionary tale? Implications for the debate on social media liability' 31.

rendering content moderation useful but flawed and only a partial solution.[205]

In addition to this, even if moderation were more reliable, it is not the primary, and certainly not the sole, factor shaping user interactions. As chapter 2 of this dissertation illustrated, features like algorithmic recommendations, interactive affordances, and user cultures contribute to users feeling comfortable behaving aggressively, viewing mis- and disinformation, disseminating it, and enabling creators to profit from it. Users spreading this information can also switch accounts or platforms when banned or when their posts are taken down.[206] However, not all users choose to do so, and those who do often lose followers and visibility.[207] In essence, determined users can generally manage to find or share disinformation, but barriers to access deprive extremists of 'two key resources: reach and attention,' making it harder to organise, access financial resources, and reach beyond existing supporters.[208]

Finally, a critique of the Information Control Approach is that it places smaller platforms at a disadvantage in an already uncompetitive market. Imposing such regulatory burdens might incur heavy costs that these platforms lack.[209] On the other hand, it is argued that these smaller platforms host significant amounts of hate speech and play a role in cross-platform extremist networks (e.g. Truth Social a social media platform created by Trump Media and Technology Group),[210] necessitating regulation.

In summary, these are the considerations that countries must take into account when choosing which approach to regulate OPM. Similar to the previous approaches, this one has its merits and demerits.

3.5 Conclusion

This chapter has examined the three primary approaches adopted by countries to regulate

[205] Zurth P, 'The German NetzDG as a role model or cautionary tale? Implications for the debate on social media liability' 35.
[206] Rutenberg I and Sugow A, 'Regulation of the Social Media in Electoral Democracies: A Case of Kenya,' 7.
[207] Rutenberg I and Sugow A, 'Regulation of the Social Media in Electoral Democracies: A Case of Kenya,' 11.
[208] Zurth P, 'The German NetzDG as a role model or cautionary tale? Implications for the debate on social media liability' 45.
[209] Rutenberg I and Sugow A, 'Regulation of the Social Media in Electoral Democracies: A Case of Kenya,' 18.
[210] Griffin R, *New School Speech Regulation (NSSR) and Online Hate Speech: A Case Study of Germany's NetzDG*, 2021, 100.

social media platforms in order to address the adverse effects of OPM within their democratic contexts. It is evident that there is no perfect regulatory solution, and each approach has its merits and flaws. This nuanced understanding is crucial as the next chapter delves into the analysis of the most suitable approach for Kenya.

4.0 THE NECESSITY OF SPECIALISED LAW TO REGULATE OPM IN KENYA

4.1 Introduction

As demonstrated in the previous chapters, OPM poses a threat to Kenya's democracy, and the existing regulatory framework has not effectively addressed this challenge. In light of these findings, this chapter examines the next steps Kenya should take. This will be done in three main parts. The first part will argue why Kenya needs specialised law to regulate OPM, while the second part will look at Kenya's distinctive regulatory and political landscape to ascertain the most fitting regulatory approach this proposed law should adopt.

4.2 The Need for Specialised Law to Regulate OPM

While there is currently no legislation in Kenya specifically addressing OPM, potential opponents of specialised laws for OPM regulation could present the following arguments. They could assert that existing laws can be broadly interpreted to regulate OPM. Alternatively, they might argue that the law can be amended to incorporate provisions regulating OPM, rendering specialised laws unnecessary. In this section, the paper will scrutinise these arguments.

4.2.1 Broad Interpretation of Existing Laws

Relying on a broad interpretation of existing laws for OPM regulation poses several challenges. For instance, there is the inherent risk that this regulatory approach may infringe upon the principle of the separation of powers, as courts potentially take on a legislative role. Following from this, numerous scholars strongly advocate for a more restrained approach, suggesting that judges should avoid extensive interpretive principles.[211] They propose that laws be applied based on their plain language whenever feasible. The reasoning behind this stance is rooted in the belief that judges, when overly focused on discerning the intent of the legislature, lack reliable methodologies to ensure the successful accomplishment of their goal.[212] And so, in practice, this tendency often becomes an excuse rather than a method for clarity. In summary, these scholars argue that a legal system should discourage judges from broadly interpreting provisions, including those related to OPM regulation, to avoid potential scrutiny for judicial activism

[211] Solan L, *The language of statutes: Laws and their interpretation,* University of Chicago Press, Chicago, 2019, 15.
[212] Solan L, *The language of statutes: Laws and their interpretation*, 15.

from scholars, citizens, and legislators.[213]

Secondly, relying on a broad interpretation of existing laws makes the legal framework reactive rather than proactive. This reactive nature implies legal precedents or regulations can only be established after a specific case is brought before the court, and even then, the precedent will only address the circumstances of that particular case.[214] For instance, if a case is presented on the role of platforms in disseminating fake news, but none of the involved parties argues that the dissemination itself is problematic, specifically when targeted at individuals likely to act on it or believe it, the court decision regulates OPM's effects rather than OPM itself.

Thirdly, the indirect application of laws, may be ineffective as some of the adverse effects of OPM may not necessarily violate any existing laws. For instance, filter bubbles are harmful, however their existence does not break any law. Therefore, the argument for relying solely on current legal frameworks, may overlook these challenges posed by OPM.

4.2.2 Amending laws

Amending laws is a complex process, and addressing the proposition that existing legislation, such as the Data Protection Act (DPA) and the Computer Misuse and Cybercrimes Act (CMCA), can be amended to incorporate regulations for OPM, reveals potential challenges. To illustrate these challenges, it is essential to understand how laws are made, particularly in the context of Kenya's legislative process.

In Kenya, the legislative process ideally begins with the formulation of policy preceding the creation of a bill or any other legislative instrument.[215] A policy serves as a guiding principle adopted or proposed by the government, party, business, or individual, outlining the general principles by which the government is guided in managing public affairs. It sets out the goals and planned activities to achieve a specific purpose.[216] Policy discussions play a crucial role in determining whether a law is necessary to achieve the aims outlined in the policy or to identify the most appropriate approach to addressing a problem or seizing an opportunity.[217]

---

[213] Solan L, *The language of statutes: Laws and their interpretation*, 16.
[214] Solan L, *The language of statutes: Laws and their interpretation*, 33.
[215] Kenya Law Review Commission, *A guide to the legislative process in Kenya*, 2015, 22.
[216] Black's Law Dictionary, 3 ed.
[217] Kenya Law Review Commission, *A guide to the legislative process in Kenya*, 2015, 24.

Laws that stem from policies are expected to align with the object and purpose of the policy.[218] Deviations from the intended purpose can result in incoherency within the legal framework. Incoherency, as referred to in this paper, signifies a situation where a provision(s) in an act significantly varies from the act's intended purpose. This becomes problematic when considering the bigger picture, as judges and legal professionals may struggle to locate relevant laws, leading to confusion within the legal system.[219] The argument here is that laws within acts should adhere to the general theme and purpose intended to maintain coherence and clarity within the legal system.

Flowing from this, this paper contends both the DPA and CMCA cannot be amended to regulate OPM. Attempting to do so would risk introducing inconsistencies within these acts, as the purposes and objectives of the DPA and CMCA may not align with the complexities and nuances associated with OPM. This will be illustrated below.

A. Examining the Limitations of the DPA Governing OPM

The creation of the DPA in Kenya was driven by the DPA policy, which aimed to give effect to Article 31 of the Constitution of Kenya 2010 that specifically addresses privacy concerns.[220] This policy highlights the Kenyan government's commitment to protecting personal data, especially personal sensitive data, and lays out the guidelines for managing it throughout its information life cycle.[221]

With this in mind, amending the DPA to incorporate regulations for OPM raises concerns about incoherency. OPM is not primarily a privacy issue, as individuals often provide consent for the utilisation of their data.[222] Instead, from insights gained in previous chapters, it is evident that OPM-related provisions aim to protect the right to free and fair elections under Article 38 of the Constitution. Thus, the divergence in objectives between the two areas could result in legislative incoherency.

In summary, the incorporation of OPM-related provisions within the DPA risks diluting the focus on privacy matters and complicating the legislation's overall coherence.

---

[218] Kenya Law Review Commission, *A guide to the legislative process in Kenya*, 2015, 24.
[219] Kenya Law Review Commission, *A guide to the legislative process in Kenya*, 2015, 25.
[220] Article 31, *Constitution of Kenya* (2010).
[221] *Data Protection Act Policy* (2018).
[222] Flaxman S, Goel S, and Rao J, 'Filter Bubbles, Echo Chambers, and Online News Consumption,' 307.

B. Examining the Limitations of the CMCA Governing OPM

The CMCA, designed primarily to address offences related to computer systems and cybercrimes, operates within a framework oriented toward criminalisation.[223] Therefore, any attempt to regulate OPM under this act would involve a criminalisation approach.

However, criminalising OPM under the CMCA would be problematic due to its potential infringement on the freedom of expression. The existing scope of the CMCA already criminalises actions such as posting or reposting fake news,[224] triggering significant apprehensions about freedom of expression in Kenya. On this, scholars argue that the act's punitive measures contribute to self-censorship among individuals and media entities to avoid potential prosecution.[225] This concern has been echoed by the High Court of Kenya in the case of *Jacqueline Okuta and another v Attorney General and 2 others (2017)*. Here, the court, in assessing the offence of publishing false information, declared it unconstitutional.[226] To arrive at this decision, the court carefully evaluated the necessity of resorting to criminal sanctions for such an offence, considering its impact on various individuals. It also explored alternative forms of punishment that could achieve the desired objective without stifling freedom of expression. The court concluded that criminalising defamation, would excessively curb the right to speak and know, emphasising that civil remedies would suffice for this, and thus a prison sentence was deemed "excessive and disproportionate to the limitation on the freedom of expression."[227] Applying the same rationale to OPM reveals the potential pitfalls of regulating OPM through criminalization. Such an approach may prompt platforms to engage in over-censorship, fearing legal repercussions.[228] In the worst-case scenario, platforms might opt to shut down operations in Kenya to evade potential prosecution.

Yet, attempting to regulate OPM under the CMCA in any other manner would be inconsistent with the primary objective of the CMCA which is to criminalise offences relating to computer systems.[229] This incongruity would result in legislative incoherency,

---

[223] Section 3, *Computer Misuse and Cybercrimes Act* (2018).
[224] Section 23, *Computer Misuse and Cybercrimes Act* (2018).
[225] Rutenberg I and Sugow A, 'Regulation of the Social Media in Electoral Democracies: A Case of Kenya,' 39.
[226] *Jacqueline Okuta and another v Attorney General and 2 others* (2017) eKLR.
[227] *Jacqueline Okuta and another v Attorney General and 2 others* (2017) eKLR.
[228] Zurth P, 'The German NetzDG as a role model or cautionary tale? Implications for the debate on social media liability,' 35.
[229] Section 3, *Computer Misuse and Cybercrimes Act* (2018).

potentially yielding an ineffective and unclear law, thereby fostering confusion and operational difficulties in Kenya's legal framework.

In summary, both the CMCA, with its current focus on criminalization, and the DPA, designed to safeguard citizens' right to privacy, prove ill-suited for regulating OPM. The CMCA's objectives, if applied to OPM, may inadvertently jeopardise freedom of expression, promote over-censorship, and introduce legislative incoherency. On the other hand, the DPA, crafted to address privacy concerns, lacks the contextual alignment needed to effectively tackle the multifaceted challenges posed by OPM.

In light of these inadequacies, there is a need for specialised legislation to govern OPM.

4.3 Considerations When Selecting the Regulatory Approach Kenya Should Take

Having established the need for specialised laws to regulate OPM in Kenya, this chapter will focus on determining a suitable approach for this legislation. As discussed in Chapter 3 of this dissertation, three regulatory approaches are available: Banning, Neutral, and Information Control. To discern which approach aligns best with Kenya's needs, three critical factors will be considered: Firstly, the legality of each approach within the Kenyan context will be evaluated. Secondly, a meticulous analysis of Kenya's political climate will be undertaken to gauge the best regulatory approach. Lastly, the impact of the approach will be analysed in light of the freedom of expression.

4.3.1 Legality of the approach

In 2010, Kenya promulgated a new Constitution, aligning itself with the global trend of constitutional reforms.[230] In Africa, this movement built upon the gains of the 1990s and aimed to ensure the internalisation and adherence to constitutional values. This constitutional phase in Africa was characterised by concerns about the perceived lack of commitment by ruling parties to new political orders, weak dedication to legal review for consistency with existing laws, and the continued violation of laws, including constitutional provisions, often with impunity.[231] In this context, the drafters of the new constitution explicitly stated in Article 2 that the Constitution is the supreme law of the

[230] Kenya Law, *The Final Report of the Constitution of Kenya Review Commission*, 2005, 11.
[231] Kenya Law, *The Final Report of the Constitution of Kenya Review Commission*, 2005, 16.

Republic, binding all persons and state organs at both levels of government.[232]

Thus, it is imperative that when a law or legislative instrument is being passed, it is in line with the Constitution and its values. In view of this, the banning approach may be ill-suited for Kenya as it has the potential to be deemed unconstitutional. Article 33 of the Constitution safeguards freedom of speech, protecting not only speakers but also the rights of individuals to "receive information and ideas," also known as the "right to receive."[233] This is crucial as access to information, particularly political information, is in the public's best interest as it fosters well-informed voting decisions among citizens.[234] Consequently, it is possible to view the receipt of these political ads as part of this right.

However, legislators may argue for the ban's justification, emphasising that freedom of speech is not absolute as Article 24 of the Constitution outlines specific conditions for limiting rights or freedoms, requiring the limitation to be lawful, necessary, and proportional.[235] Additionally, legislators must consider the relationship between the limitation and its purpose, as well as explore whether there are less restrictive means to achieve the intended purpose.[236]

A blanket ban on all political advertisements on social media platforms might struggle to meet the criteria related to the "relationship between the limitation and its purpose" and the exploration of "less restrictive means." This is because this test demands that the regulation be only as extensive as necessary, requiring a reasonable "fit" between the legislative means and ends.[237] While it doesn't mandate the least restrictive way, a ban on all political advertising would likely be deemed more extensive than necessary, resulting in the loss of all benefits associated with OPM. Thus, this leaves us with two alternative approaches to consider.

The neutral and information control approaches, unlike the banning approach, pass the legality test. This is because both approaches allow for OPM just requiring that its effects

[232] Article 2, *Constitution of Kenya* (2010).
[233] Sugow A, 'The Right to be Wrong: Examining the (Im) possibilities of Regulating Fake News while Preserving the Freedom of Expression in Kenya' 1 *Strathmore Law Review* 1, 2019, 17.
[234] Article 33, *Constitution of Kenya* (2010). See also Article 19, *International Covenant on Civil and Political Rights,* 1 May 1972, 999 UNTS 171.
[235] Article 24, *Constitution of Kenya* (2010).
[236] Article 24, *Constitution of Kenya* (2010).
[237] Sugow A, 'The Right to be Wrong: Examining the (Im) possibilities of Regulating Fake News while Preserving the Freedom of Expression in Kenya,' 14.

be mitigated.

4.3.2 Elections, Manipulation, and the Regulation of OPM

The next step in determining the most effective approach for Kenya to regulate OPM is a thorough examination of the country's political climate. However, understanding the political context in Kenya requires tracing back to its independence.

In 1964, Kenya became a republic, with Jomo Kenyatta becoming the first President.[238] However, a disagreement between Kenyatta and his first vice president led to the formation of the rival Kenya People's Union (KPU) party. This move solidified the ethnic divisions along party lines, particularly between the Kikuyu majority supporting KANU and the Luo supporting KPU, leaving a lasting impact on the political landscape.[239]

The next significant milestone occurred in 1969 when KPU was banned, effectively making Kenya a de facto one-party state under KANU.[240] This single-party dominance endured throughout the 1980s, as Kenya even officially became a de jure one-party state in 1982. The landscape, however, witnessed a transformative shift in 1991, marking the end of the one-party rule. Despite this political evolution, the event underscored the extent to which candidates were prepared to go to secure electoral victories, revealing instances of abuse of power and signs of dictatorship.[241]

Subsequently, the elections in 1992 and 1997, despite Kenya's multi-party status, failed to meet international democratic standards, with clear indications of vote theft.[242] These elections heightened tensions and hostilities in Kenya, particularly along tribal lines. The culmination of these tensions occurred in the 2007 post-election violence, resulting in the loss of lives and displacement of hundreds of thousands of people.[243] The violence stemmed from voter dissatisfaction with election manipulation, ethnic divisions, and rallying and incitement by political parties and leaders.[244]

Since then, in the 2017 and 2022 elections, while violence has not occurred, political

[238] Administration and Cost of Elections Project, *KENYA ELECTION HISTORY 1963-2013*, 2014, 1.
[239] Administration and Cost of Elections Project, *KENYA ELECTION HISTORY 1963-2013*, 2014, 1.
[240] Administration and Cost of Elections Project, *KENYA ELECTION HISTORY 1963-2013*, 2014, 7.
[241] Administration and Cost of Elections Project, *KENYA ELECTION HISTORY 1963-2013*, 2014, 10.
[242] Administration and Cost of Elections Project, *KENYA ELECTION HISTORY 1963-2013*, 2014, 11.
[243] Administration and Cost of Elections Project, *KENYA ELECTION HISTORY 1963-2013*, 2014, 16.
[244] Administration and Cost of Elections Project, *KENYA ELECTION HISTORY 1963-2013*, 2014, 19.

parties persist in employing various means, as highlighted in Chapter 2, such as PM and OPM, to secure their victories. Therefore, Kenya's chosen regulatory approach should take into account the historical context of election manipulation, ethnic divisions, and the influence wielded by political parties and leaders.

Bearing this in mind, the neutral approach might be insufficient in regulating OPM in Kenya. This approach, as mentioned earlier, allows OPM but demands strict disclosure and transparency from platforms. Under this approach, social media platforms are expected to take measures for accessibility, due diligence, privacy, and transparency. Safe harbour provisions are then granted to them if they do so, based on the assumption that economic self-interest will drive self-regulation.

However, in Kenya, this approach falls short because platforms lack the incentive to mitigate election manipulation. Instead, they are more incentivised to engage in OPM, using it to boost user engagement through the dissemination of fake news and political ads. This is because this content generates extreme reactions that boost user engagement for platforms through likes, comments, and shares.[245] Moreover, political ads serve as a substantial revenue source for platforms during elections, creating financial incentives for their involvement in OPM. In the 2022 elections alone, the estimated cost of presidential campaigns reached Ksh.36 billion.[246] While not all of this funding went directly to OPM, it underscores candidates' financial capacity to fund such activities and pay platforms for their services. Consequently, platforms are more inclined to engage in OPM than to self-regulate against its negative consequences.

Consequently, the information control approach emerges as the most viable option for OPM regulation in Kenya. The biggest critique of this approach, however, is that it infringes on freedom for expression.

[245] Allcott H and Gentzkow M, 'Social Media and Fake News in the 2016 Election,' 213.
[246] https://www.standardmedia.co.ke/article/2000074352/campaigns-could-cost-sh36-billion on 25th January 2024.

4.3.3 Weighing the Freedom of Expression

When implemented in other countries, the information control approach has faced criticism for its perceived encroachment on freedom of expression. This criticism stems from two key factors. Firstly, there is concern about potential bias leading to excessive content removal, thus raising concerns about the infringement on freedom of expression.[247] Secondly, the privatisation of enforcement raises apprehension about freedom of expression, as platforms, rather than courts or democratically legitimized institutions, assess the legality of content. [248]

This potential to limit freedom of expression in Kenya is particularly concerning due to the history of abuse of this freedom. For instance, during Moi's era in 1982, the New York Times reported that three editors and two reporters from Eastern Africa's largest newspaper group were detained and tortured by the police for merely critiquing the government.[249] And this was not all. The President further threatened to shut down the newspapers for merely publishing this content. This was just one of several instances during this period when people were detained for expressing themselves. Then, even in Kibaki's era, attempts to suppress press freedom were evident, such as the police raid on Standard Media in 2006.[250] Here, 30 hooded members of the police unit raided Standard media. The police raid followed a dispute between the standard media house and the government over a story in that week's Sunday Standard alleging that President Kibaki had held a secret meeting with one of his biggest critics, former cabinet minister Mr. Kalonzo Musyoka. Additionally, two days prior to this attack, three of the journalists were seized and held in police custody over the story.

Post the 2010 constitution, laws that limit freedom of expression, including measures to take down fake news, have generally faced resistance in courts. For instance, in the case *Alai v. Attorney General* the court emphasised that the people of Kenya "have a democratic right to discuss affairs of their government and leadership because of their right to freedom of expression and [t]hey cannot be freely expressing themselves if they

[247] Griffin R, *New School Speech Regulation (NSSR) and Online Hate Speech: A Case Study of Germany's NetzDG*, 2021, 47.
[248] Griffin R, *New School Speech Regulation (NSSR) and Online Hate Speech: A Case Study of Germany's NetzDG*, 2021, 50.
[249] https://www.nytimes.com/1981/05/23/world/kenya-said-to-detain-5-journalists.html on May 23 1981.
[250] https://humanrightshouse.org/articles/kenya-armed-police-attack-and-shut-down-newspaper-and-tv-station/ on March 2 2006.

do not criticize or comment about their leaders and public officers."[251] Using this reasoning, arguments could be made in favour of fake news, suggesting that fake news is a form of criticizing the government.

Consequently, for Kenya to regulate OPM through the information control approach, any limitation on freedom of expression must align with the constitutional provisions and be justified. As per Article 24 of the Constitution, limitations on rights or freedoms should be lawful, necessary, and proportional. The relationship between the limitation and its purpose must be considered, along with exploring less restrictive means.

In this context, regulating OPM is lawful, necessary, and proportional as it safeguards the right to free and fair elections.[252] The scale and technical operations of online platforms make it impractical for state institutions to handle first-instance moderation decisions, justifying the delegation of enforcement to platforms.[253] Furthermore, this approach minimizes the risk of manipulation by the ruling party, ensuring that content removal policies are not unilaterally dictated by the government, thereby mitigating the potential for abuse of power, a concern that has been evident in Kenya. Moreover, this approach satisfies the criterion of having no less restrictive means to achieve its purpose. As discussed earlier, the banning approach could likely be deemed unconstitutional, as it foregoes the benefits associated with OPM, while the neutral approach falls short of effectively safeguarding against manipulation through OPM. Hence, the information control approach stands out as the most suitable in this context.

Lastly, the information control approach is especially well-suited for Kenya's context as it actively addresses the issue of filter bubbles. By regulating the criteria under which a person can be targeted, this approach becomes crucial in countering filter bubbles and mitigating their potential harm. This is particularly important given Kenya's susceptibility to abuses based on ethnic considerations, as illustrated above.

4.4 Conclusion

This chapter has emphasised the necessity of enacting specialised law to address the

[251] *Alai v Attorney General* (2017) eKLR.
[252] Article 38, *Constitution of Kenya* (2010).
[253] Griffin R, *New School Speech Regulation (NSSR) and Online Hate Speech: A Case Study of Germany's NetzDG*, 2021, 48.

challenges of OPM in Kenya. Acknowledging the historical context of the constitution, ethnic divisions, election manipulation, and the potential for abuse of power, a nuanced regulatory approach becomes paramount. The information control approach emerges as a robust recommendation, actively tackling the persistent issues of OPM and shortcomings associated with a neutral stance.

5.0 CONCLUSION

This study has been instigated by the prevalent use of OPM in Kenyan politics, recognizing its potential risks to the democratic process. Throughout this research, the primary focus has been on assessing the threat posed by OPM and exploring ways to effectively regulate and mitigate its adverse effects. The preceding chapters have delved into understanding the complexities surrounding OPM, examining its impact on democracy, illustrating the inadequacies of existing regulatory frameworks, and proposing the need for specialised legislation. This concluding chapter aims to present the key findings, tie them back to the initial objectives, and present recommendations for addressing the challenges posed by OPM.

5.1 Summary of findings

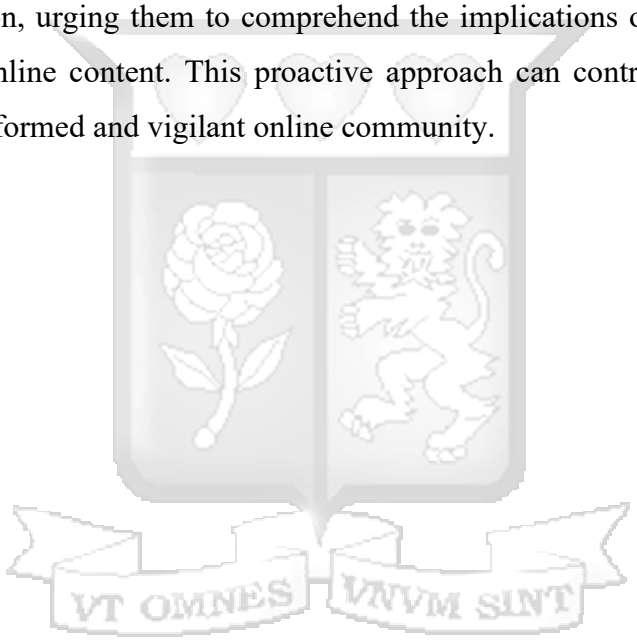
The overarching objective of this study was to comprehensively grasp and tackle the challenges presented by OPM in Kenya. The preceding chapters accomplished this objective. In Chapter One, the research was introduced, laying out research questions, a conceptual framework, and the design of subsequent chapters. Chapter Two provided a definition of OPM, illustrating its adverse effects on democracy in Kenya and highlighting the shortcomings of existing regulations. Chapter Three conducted a critical assessment of the three global regulatory approaches to OPM, exposing their limitations and establishing a foundation for the following chapter. Chapter Four expanded on these insights, advocating for specialised legislation to address these challenges. To arrive at this, it explored the inadequacies of relying on broad interpretations or amendments to existing laws, concluding that Kenya needed specific legislation for effective regulation. To determine the appropriate approach for this specialised law, the chapter scrutinised Kenya's political landscape, suggesting the information control approach as the most suitable. Consequently, Chapter Five aims to outline both legal and non-legal recommendations based on the research findings.

5.2 Recommendations

In light of the identified risks and challenges associated with OPM in Kenya, this study puts forward the following legal and non-legal recommendations.

From a legal perspective, it is strongly advised that the government institute specialised legislation to regulate social media platforms, mitigating the potential adverse effects of OPM. Drawing inspiration from successful models such as the NetzDG and Digital Services Act, this legislation should adopt the information control approach. To bolster the effectiveness of regulatory measures, it is further recommended that this legislation incorporates stringent penalties for non-compliance with OPM regulations. These penalties are essential as deterrents, discouraging entities from engaging in the misuse of OPM.

On the non-legal front, the government and civil society organisations should initiate comprehensive awareness campaigns to educate citizens about the effects of OPM. These campaigns should empower citizens with knowledge about the potential consequences of online manipulation, urging them to comprehend the implications of their consent when interacting with online content. This proactive approach can contribute significantly to building a more informed and vigilant online community.



BIBLIOGRAPHY

Books

Ghonim W, *Revolution 2.0: The Power of the People Is Greater Than the People in Power: A Memoir*, Houghton Mifflin Harcourt, Egypt, 2012.

Morozov E, *The Net Delusion: The Dark Side of Internet Freedom,* PublicAffairs Books, New York, 2014.

Pariser E, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think,* Penguin Publishing Group, London, 2011.

Sunstein C, *Republic: Divided Democracy in the Age of Social Media*, Princeton University Press, New Jersey, 2017.

Chapter in Books

Benjamin S, 'The First Amendment and Algorithms' in Woodrow Barfield (ed) *The Cambridge Handbook of the Law of Algorithms*, Cambridge University Press, New York, 2021, 606-631.

Journal Articles

Acerbi A, 'Cognitive Attraction and Online Misinformation' 5 *Palgrave Communications* 1, 2019.

Allcott H and Gentzkow M, 'Social Media and Fake News in the 2016 Election' *31 Journal of Economic Perspectives* 2, 2017.

Awad J and Krishnam M, 'Social Media and Its Role in Political Campaigns: A Review of Literature' *University of Pennsylvania Press*, 17 Aug 2020—https://knowledge.wharton.upenn.edu/podcast/knowledge-at-wharton-podcast/how-social-media-is- shaping-political-campaigns/.

Bozdag E and Van Den Hoven J, 'Breaking the filter bubble: democracy and design' 17 *Ethics and information technology* 1, 2015.

Bulka T, ‘Algorithms and Misinformation: The Constitutional Implications of Regulating Microtargeting' 32 *Fordham Intellectual Property, Media and Entertainment Law Journal* 4, 2022.

Casagran C and Vermeulen M, "Reflections on the murky legal practices of political micro-targeting from a GDPR perspective’ 11 *International Data Privacy Law* 4, 2021.

Citron D and Benjamin W, ‘The internet will not break: Denying bad Samaritans section 230 immunity’ 1 *Fordham Law Review* 86, 2017.

Couzigou I, ‘The French Legislation Against Digital Information Manipulation in Electoral Campaigns: A Scope Limited by Freedom of Expression’ 20 *Election Law Journal: Rules, Politics and Policy 1,* 2021.

Dobber T, Fathaigh R and Borgesius F, ‘The regulation of online political micro-targeting in Europe’ 8 *Internet Policy Review* 4, 2019.

Dommett K, 'Data-driven political campaigns in practice: understanding and regulating diverse data- driven campaigns' 8 *Internet Policy Review* 4, 2019.

Farkas J, ‘Fake News in Metajournalistic Discourse’ 24 *Journalism Studies* 4, 2023.

Flaxman S, Goel S, and Rao J, ‘Filter Bubbles, Echo Chambers, and Online News Consumption’ 80 *Public Opinion Quarterly* 1, 2016.

Frederik J, Zuiderveen B, Möller J, Kruikemeier S, Fathaigh R, Irion K, Dobber T, Bodo B, and Vreese C, 'Online Political Microtargeting: Promises and Threats for Democracy' *Utrecht Law Review,* 2018.

Heldt A, ‘Reading between the lines and the numbers: an analysis of the first NetzDG reports’, 8 *Internet Policy Review* 2, 2019.

Hoegg J and Lewis M. ‘The Impact of Candidate Appearance and Advertising Strategies on Election Results’ 48 *Journal of Marketing Research* 5, 2011.

Holt K, Shehata A, Strömbäck J, and Ljungberg E, ‘Age and the effects of news media attention and social media use on political interest and participation: Do social media function as leveller?’ 1 *European journal of communication*, 1, 2013.

Jamieson K, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President—What We Don't, Can't, and Do Know,* Oxford University Press, New York, 2018, 88.

Kirdemir B, 'Exploring Turkey's Disinformation Ecosystem' *Centre for Economics and Foreign Policy Studies,* 2020 - https://www.jstor.org/stable/resrep26087.

Korolova A, 'Privacy Violations using Microtargeted Ads: A Case Study' 3 *Journal of Privacy and Confidentiality* 1, 2011.

Kosinski M, Stillwell D and Graepe T, 'Private Traits and Attributes are Predictable from Digital Records of Human Behavior' 110 *Proceedings of the National Academy of Sciences of the United States of America* 15, 2013, 31.

Leerssen P, Ausloos J, Zarouali B, Helberger N, and de Vreese C. H., 'Platform ad archives: promises and pitfalls' 8 *Internet Policy Review* 4, 2019.

Mude H, 'Political Micro-Targeting in Kenya: An Analysis of the Legality of Data Driven Campaign Strategies under the Data Protection Act' 1 *Journal of Intellectual Property and Information Technology Law* 1, 2021.

Muthuri R, Karanja M, Monyango F and Karanja W, 'Investigating privacy implications of biometric voter registration In Kenya's 2017 election Process' 1 *Centre for Intellectual Property and Information Technology Law* 1, 2018.

Mutung'u, G, 'The Influence Industry Data and Digital Election Campaigning in Kenya' 1 *Our Data Ourselves* 1, 2018.

Nott L, 'Political Advertising on Social Media Platforms' 45 *American Bar Association Journal* 3, 2020.

Nyhan B and Reifler J, 'When corrections fail: The persistence of political misperceptions' 32 *Political Behavior* 2, 2010.

Phillips C, 'The Regulation of Public Utilities' 2 *Technology and Investment Journal* 1, 2010.

Rutenberg I and Sugow A, 'Regulation of the Social Media in Electoral Democracies: A Case of Kenya' 8 *Journal of African Law* 1, 2020.

Schulz W, 'Regulating intermediaries to protect privacy online–the case of the German NetzDG', *Personality and Data Protection Rights on the Internet*, 8 March 2021 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3216572 .

Solan L, *The language of statutes: Laws and their interpretation,* University of Chicago Press, Chicago, 2019.

Sugow A, 'The Right to be Wrong: Examining the (Im) possibilities of Regulating Fake News while Preserving the Freedom of Expression in Kenya' 1 *Strathmore Law Review* 1, 2019.

Tufekci Z, 'Twitter and Tear Gas: The Power and Fragility of Networked' 38 *Strategic Studies* 3, 2018.

Vold K and Whittlestone J, 'Privacy, autonomy, and personalised targeting: rethinking how personal data is used' *Leverhulme Centre for the Future of Intelligence*, 2019, 6 - http://lcfi.ac.uk/resources/privacy-autonomy-and-personalised-targeting-rethin/ - on 13 January 2023.

Wanyama F, Elkit J, Frederiksen B and Kaarsholm P, 'Ethnicity and/or Issues? The 2013 General Elections in Western Kenya' 13 *Journal of African Elections* 2, 2014.

Yerlikaya T and Aslan S, 'Social Media and Fake News in the Post-Truth Era: The Manipulation of Politics in the Election Process' 22 *Insight Turkey* 2, 2020.

Zarouali B, Dobber T, and Schreuder J, 'Personality and susceptibility to political microtargeting: A comparison between a machine-learning and self-report approach' 151 C*omputers in Human Behavior* 4, 2023.

Zarouali B, Dobber T, De Pauw G, and de Vreese C, 'Using a Personality-Profiling Algorithm to Investigate Political Microtargeting: Assessing the Persuasion Effects of Personality-Tailored Ads on Social Media,' 49 *Communication Research* 8, 2022.

Zurth P, 'The German NetzDG as a role model or cautionary tale? Implications for the debate on social media liability' 4 *Fordham Intellectual Property Media & Entertainment. Law Journal* 1, 2020.

Reports and Institutional Authors

Administration and Cost of Elections Project, *KENYA ELECTION HISTORY 1963-2013*, 2014.

Amnesty International's report, *Tear Down This Wall: The Anatomy of Facebook's Role in the Myanmar Genocide*, 2020.

Article 19, *Germany: Responding to Hate Speech. Country Report*, 2018.

Deloitte, *Cookies bench study,* 2020.

Global Web Index, *Social Media Statistics*, 2023.

Griffin R, *New School Speech Regulation (NSSR) and Online Hate Speech: A Case Study of Germany's NetzDG*, 2021.

Institute for Free Speech, *The Truth About "Microtargeting" and Political Speech: Why a Ban Is a Bad Idea,* 2021.

Kenya Law, *The Final Report of the Constitution of Kenya Review Commission*, 2005.

Kenya Law Review Commission, *A guide to the legislative process in Kenya*, 2015.

Rand corporation, *Hostile Social Manipulation: Present Realities and Emerging Trends*, 2019.

Statista, *Number of social media users in Kenya from 2014 to 2022*, 1 Aug 2022.

Transatlantic Working Group, *An Analysis of Germany's NetzDG Law,* 2019.

University of Oxford, *The Reuters Institute Digital News Report,* 2021.

Working Papers, Discussion Papers and Research Papers

Geddes R, 'Public Utilities' Cornell University, Working Paper, 1998 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=92688.

Tworek H and Leerssen P, 'An Analysis of Germany's NetzDG Law' University of Amsterdam, Transatlantic Working Group Working Paper, 2019 -

https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Le.

Dissertations and Theses

Griffin R 'New School Speech Regulation (NSSR) and Online Hate Speech: A Case Study of Germany's NetzDG', Unpublished Thesis, Hertie School, Berlin, 2021, 53.

Other internet sources

Bartlett A, 'Different Strokes: Political and Economic Systems Around the Globe' Lumen learning, February 12 2021 https://courses.lumenlearning.com/suny-internationalbusiness/chapter/reading-capitalism-in-the-us/#:~:text=Democratic%20capitalism%2C%20also%20known%20as,predominantly%20on%20a%20democratic%20polity.

Cakebread C, 'You're not alone, no one reads terms of service agreement', Business Insider, 15 November 2017 https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11?r=US&IR=T.

Cohen J, 'It Would Take 17 Hours to Read the Terms & Conditions of the 13 Most Popular Apps' PC gamer Newsletter, 4 December 2020 https://www.pcmag.com/news/it-would-take-17-hours-to-read-the-terms-conditions-of-the-13-most-popular.

Granville K, 'Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens' The New York Times, 4 April 2018 https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica- scandal-fallout.html.

Hayes A, ' What Is a Safe Harbor? Types, and How They Are Used' Investopedia, November 21 2020

https://insights.advocates.ke/legal-reforms-kenya-can-borrow-to-regulate-microtargeting/.

https://www.facebook.com/business/news/bringing-more-transparency-to-political-ads-

in-2019.

https://www.investopedia.com/terms/s/safeharbor.asp.

https://www.standardmedia.co.ke/article/2000074352/campaigns-could-cost-sh36-billion

Khan C, 'Despite report findings, almost half of Americans think Trump colluded with Russia' Reuters, March 27 2019 https://www.reuters.com/article/idUSKCN1R72SJ/.

Koebert J, 'Cookies Study: 40% of Americans Blindly Accept Internet Cookies, But Most Don't Know What They Do' 21 September 2023 https://allaboutcookies.org/internet-cookies-survey.

Madung O, 'From Dance App to Political Mercenary: How disinformation on TikTok gaslights political tensions in Kenya' *Mozilla Report*, 2022, 14 - https://foundation.mozilla.org/en/campaigns/kenya-tiktok/ on 9 January 2024.

Olivia L, 'Disinformation was rife in Kenya's 2022 election', Africa at LSE, January 5 2023 https://blogs.lse.ac.uk/africaatlse/2023/01/05/disinformation-was-rife-in-kenyas-2022-election/.

Papadopoulos P, Markatos E, Kourtellis N, 'Cookie Synchronisation: Everything You Always Wanted to Know But Were Afraid to Ask,' Research Gate, 13 May 2018, 14 https://dl.acm.org/doi/abs/10.1145/3308558.3313542#:~:text=Cookie%20Synchronization%20work%3F-,Cookie%20Synchronization%3A%20Everything%20You%20Always%20Wanted%20to,But%20Were%20Afraid%20to%20Ask&text=User%20data%20is%20the%20primary,to%20data%20markets%20and%20advertisers.

Thomas K, Grier C and Nicol D, *'Unfriendly: Multi-party Privacy Risks in Social Networks'*, Springer Berlin Heidelberg, 21 May 2010, 237 https://link.springer.com/chapter/10.1007/978-3-642-14527-8_14.

Vote Leave's targeted Brexit ads released by Facebook' BBC News, 26 July 2018 https://www.bbc.com/news/uk-politics-44966969.

Wakabayashi D, 'Russian Influence Reached 126 Million Through Facebook Alone', The

New York Times, October 30 2017 https://perma.cc/5X63-VM62.

Wamuyu P, 'Social Media Consumption Among Kenyans: Trends and Practices' IGI Global, 2020, 23 https://doi.org/10.4018/978-1-7998-4718-2.ch006.

Witte M, 'Four questions: Evelyn Douek, on what Section 230 is and why it is misunderstood', Stanford News, 7 October 2022 https://news.stanford.edu/2022/10/07/four-questions-evelyn-douek-section-230-misunderstood/.

'Google customer match help' https://support.google.com/adspolicy/answer/6299717?hl=en.

'How to use Facebook custom audiences' https://support.google.com/adspolicy/answer/6299717?hl=en.

'Tailored audiences' https://business.twitter.com/en/help/campaign-setup/campaign-targeting/custom-audiences.html.

Dictionaries and Encyclopaedias

Black's Law Dictionary, 3 ed.

Merriam Webster Dictionary, 4 ed.