Online safety in Kenya: A snapshot of the Silicon Savannah

Sylvia Ndanu Mutua[1] and Zhang Kai[2]
[1]**Department of Communication Studies, Technical University of Mombasa, P.O. Box 90420 – 80100, Mombasa, Kenya**.
[2]Institute of Communication Studies, Communication university of China, No.1 Dingfuzhuang East Street, Chaoyang District, Beijing, P. R. China 100024.

Author's email: smutua2014@tum.ac.ke

Abstract

This article provides an overview of online safety in Kenya by outlining key threats and the interventions that have been implemented to combat these threats. Using the social responsibility theory, this article further explores internet users' perceptions of online social responsibility in cyberspace. Results of the study indicate that the internet media environment which is characterized by interactivity significantly moderates the internet users' perception of their online social responsibility. However, despite the court suspensions of some of the laws, the existing online content regulations still have a significant influence on online safety. Consequently, the article advocates the need to associate the concept of human dignity with the responsibilities that each person must take for his or her online actions. This implies that one's online dignity would entail one owning up to their online conduct in the quest for safe, respectful, inclusive, and harmonious cyberspace. Also, greater online social responsibility by Kenyan internet users would be necessary to foster free speech, open access, and a social culture of respecting others, and not harming others in cyberspace.

Key Words: Online content regulation, Online Safety, Social responsibility, Internet users, Kenya

Introduction

In recent years scholars, educators, government institutions, and the media have raised concerns over the ever-increasing online risks that internet users face in the ever-evolving internet ecosystem. This has necessitated calls for suitable measures to be put in place to abate online harm. According to De Kimpe et al. (2019), these online safety measures have often been referred to as internet safety, e-Safety, or digital safety. Additionally, they incorporate several issues that are both directly or indirectly related to the psychological and physical well-being of internet users. Tsai et al. (2016) further note that the online safety discourse is concerned with the online risks that individuals may face and the measures they can take to protect themselves from those risks.

Some authors (Macaulay et al., 2020; Pinter et al., 2017; Wisniewski, 2018) have examined the concept of online safety from the perspectives of adolescents and young children. This is because young people especially adolescents have been known to be the most active in cyberspace, especially on social media platforms (Odgers et al., 2020). However, Mazur et al. (2019) note that the focus on online safety studies on children and adolescents does not imply that older people are not susceptible to online risks. Although adults may have a lower probability to engage in risky online behavior, they are no exception to the potentially negative effects related to being in the cyber environment such as; believing fake news and disinformation, reputational damage, or being conned through online scams.

Several initiatives have been implemented by governments across the world in promoting the online safety of internet users in their jurisdictions (You & Zhengxu, 2020). Some of these measures have included internet shutdowns and legislation policies implemented at the national level by governments in their respective jurisdictions. Other governments have also partnered with internet-related corporate organizations such as Google and Meta Platforms, Inc. to advance other online safety

Published, January 2023

initiatives focusing on the empowerment of internet users (Vraga et al., 2020). Some of these initiatives have recorded significant success especially in curbing illegal and harmful online content and enforcing online child protection. However, more still needs to be done in making cyberspace a safer space without compromising fundamental human rights.

Given the above, this study sought to examine the present realities concerning online safety in Kenya. This is an East African country commonly known as the Silicon Savannah due to its thriving technology scene that is home to the most cutting-edge start-ups on the African continent. Focusing on online content on social media platforms, this study sought to examine the opinions of Kenyan internet users regarding online safety and if existing online content legislation has had any effect on the advancement of online safety in Kenyan cyberspace.

Overview of Kenyan cyberspace

Kenya boasts of an ICT-connected landscape characterized by being among the sub-Saharan African countries with the fastest mobile internet speeds due to its undersea fiber optic cables. As of June 30, 2021, the Cable.co.uk organization posted on its website the Worldwide broadband speed league 2021 report, where they noted that Réunion had the highest mean download speed (Mbps) of 43.62.87 Mbps in Sub-Saharan Africa, while Kenya took sixth place with 11.27 Mbps. Admittedly, its $1 billion technology ecosystem offers an attractive space for investors, entrepreneurs, and technologists. Established firms such as; Microsoft, Facebook, Intel, and IBM have found a home in this cradle of innovation. As the East Africa region's hub for communication, transportation, and financial services, the Kenyan Government regards ICT innovations and technologies as key enablers in the transformation of the nation and the achievement of a digital economy. This is documented in the national development plan of Vision 2030 (Ministry of Devolution and Planning, 2013). Kenya is also a strong contender for early 5G deployment, given its emphasis on cultivating a digital-based economy. However, like other countries across the globe Kenya, has greatly been affected by the rise in illegal online content and irresponsible user behavior in its cyberspace. According to the national ICT regulator namely, the Communication Authority of Kenya (CA), cyber threats rose by over 10% in the first quarter of 2019 (Adonija, 2019; Wainaina, 2019). The impact of these online risks is further noted by Oluoch (2019) and Wamuyu (2020) who note that on an average day, three to five Kenyans have reported suffering inconvenience and psychological harm because of individual cyber threats on social media platforms.

In response to the evolving online content threats and in an attempt to protect its citizenry, the Kenyan Government has instituted several legislations to promote online safety and curb illegal online content and irresponsible internet user behavior. These provisions are contained in legislation policies which include; the Constitution of Kenya 2010, The Kenya Information and Communication Act No. 2 of 1998, the Computer Misuse and Cyber Crimes Act No. 5 of 2018, and the Data Protection Act No. 24 of 2019. Although the Computer Misuse and Cybercrimes Act 2018 does not explicitly define what online safety entails, it describes several online offenses with some being concerned with online content. For example, Sections 22 and 23 of the Computer Misuse and Cybercrimes Act 2018 refer to false publications and fake news as offenses. Other sections outline offenses concerned with internet user behavior such as; Section 24 on Child pornography, Section 27 on cyber harassment, cyber espionage under Section 21 as well as phishing in Section 30 among others.

Online content regulation challenges

One of the major challenges regarding the regulation of online content in most sub-Saharan African countries is the foreign element that characterizes Over-the-Top providers (OTTs). Most of the OTTs are registered and have their headquarters based abroad but they provide services to the entire world. These OTTs have a substantial presence and contact with the Kenyan cyberspace where they do their businesses and this has resulted in conflict between them and some of the local telecommunication companies. The local telecommunication companies argue that these applications are not only usurping their revenues but also pose a national security threat (Stork & Esselaar, 2019). Additionally, Bernard (2016) argues that challenges still arise

on how best to address disputes that arise over internet issues, with no consistent legislative standard for how to apply traditional notions of personal jurisdiction to cyberspace cases. World Economic Forum (2019) noted that among the technological vulnerabilities, most people have encountered risks associated with fake news and identity theft as well as loss of privacy to companies and governments across different jurisdictions.

Online content definitional challenges

As governments institute legal interventions to counter online content threats, challenges arise, in coming up with clear definitions between online content that is illegal and online content that is harmful but not necessarily illegal. A recent example of this challenge was exemplified in the 2019 UK online harms white paper which outlined the approach of the UK Government in addressing online activity and content that is a threat to the United Kingdom's way of life or poses harm to individual internet users, especially children. The paper recommended a single regulation framework, with its core being a legislative duty of care obligatory for internet corporations as well as social media platforms (Wright & Javid, 2019). However, authors (Barker & Jurasz 2019; Tambini, 2019) have highlighted regulatory challenges of the white paper which partly emanate from the unhelpful distinction between illegal online content and harmful but not illegal online content. As such, they posited that these different categories of online content by not legally having the same meaning should not be subjected to the same regulatory standards. On the other hand, although social media platforms do not explicitly define content as illegal; they have imposed comparable restrictions on their subscribers through their community standards and service specifications by outlining the content that is not allowed on their platforms.

For example, on the Facebook platform, the subscribers must adhere to the community standards that are predefined on content such as cyberbullying, cyber threats, nudity, graphic violence, the sale, and procurement of sex services, and prohibited goods (Facebook, 2017). On the Twitter platform, they have a user agreement that also forbids among other issues, hateful and abusive content, unauthorized sharing of intimate media or private information of another person as well as internet protocol violations (Twitter Help Center, 2019). Although some of these regulations attempt to distinguish acceptable online content from harmful or illegal content; they are at times also socially constructed by broader universality on some socio-cultural norms especially as it regards online content that is deemed inappropriate and/or offensive. This is exemplified in Facebook regulations regarding sexualized content and nudity. The categorizations were not adopted from laws on obscenity but rather emanated from internet users' apprehensions about exposing minors to online content that was considered inept and unacceptable (Yar, 2018).

Kenya like most other countries does not have a clear explicit definition of illegal and harmful content. However, any type of content that is identified and described in the various laws and policies as constituting an offense is regarded as illegal. In this study, we define illegal online content and irresponsible user behavior to constitute online content and behavior that fits the description in the categories of offenses in the Computer Misuse and Cybercrime Act 2018. This content includes false publications, false information, child pornography, cyber terrorism, and the wrongful distribution of obscene or intimate images. Hate speech which is an offense under the National Cohesion and Integration Act 2008 also forms part of our classification of illegal online content. Irresponsible user behavior, which contributes to harmful content posted toward another user, such as cyber harassment is also considered part of the study.

Online Social responsibility

The social responsibility theory by, Siebert et al. (1956) is premised on the fact that freedom should come with responsibility. In dealing with user-generated content in cyberspace, there is a need to make a clear distinction between responsibility, accountability, and liability. Plaisance (2013) in distinguishing between accountability and responsibility defined the latter as a recognized obligation for conduct within contexts of roles and moralities in a particular situation, while this author denoted accountability as the demonstration of assertions

of obligation. This implies that responsibility is more of a claim of taking the interests and safety of one's audience as of paramount importance. More specifically, looking at the cyberspace setting, social responsibility would entail the necessity for internet users to hold societal interests in high regard. This can be regarded as a communal responsibility in the public interest. The cyberspace environment, through social media platforms, has so far distinguished itself not just as a means of transmitting information but also as a new communication sphere. Its interactive nature has afforded the public a two-way communication structure different from that of the mass media which was described by a linear structure.

There have been several calls for internet users to be socially responsible for their conduct in cyberspace environment. Cohen-Almagor (2017) in advocating for online safety distinguished between the terms Net user and Net citizen based on the level of social responsibility of the ideal participants in cyberspace. He noted that net users were simply individuals who used the Internet, without conveying either the how of their usage or appraising their utilization of it. On the other hand, net citizens referred to an appraisal of a user's responsible use of the internet. These ideal net citizens would suggest individuals who use the Internet as an integral part of their real life. Implying that their virtual life is not separated from their real life. Subsequently, if they invent an identity for themselves on social networks, they do it responsibly, holding themselves accountable for the consequences of their Internet use (Cohen-Almagor, 2017).

As a theory that lies between the two extremes of the authoritarian theory and the libertarian theory; social responsibility theory is very significant in online safety research because it acknowledges the internet user as a crucial agent concerning online safety in cyberspace. This is because the internet user despite having the freedom to create, receive, and share online content, is also affected by several external controls. These external controls include other internet users, social media platform companies, and the government regulations in place. Moreover, the theory also inspires aspects of self-control in internet users, thereby instilling a sense of responsibility, accountability, and liability for their online conduct for the good of the cyber ecosystem.

Given the above context, this study sought to answer; 1) what online content threats affect online safety in Kenyan cyberspace, and 2) what interventions are being implemented to advance online safety within Kenyan cyberspace.

Methodology

Data Collection and Analysis

The study examined the perceptions of Kenyan social media users by exploring the relationship between the existing online content regulations and online safety, by testing the following hypotheses;

1. **H_1**: The existing online content regulatory policies significantly influence online safety in Kenyan cyberspace
2. **H_2**: Internet user perceptions of social responsibility moderates the effect of existing content regulatory policies in promoting online safety in Kenyan cyberspace
3. **H_3**: Online media environment moderates the effect of existing content regulatory policies in promoting online safety in Kenyan cyberspace

The data collected for this study was both quantitatively and qualitatively analyzed. Quantitative data was collected through a web-based survey comprising both open-ended and Likert scale responses. Participants were sent a web link to the survey and assured that their responses would be anonymous, as no identifying data was being collected. Qualitative data emanated from Facebook social media posts and in-depth interviews with government officials working in government regulatory agencies. Data from the Facebook social media platform was collected using crowd tangle software for a period between November 2019 and November 2020.

The publicly available social media posts were used to analyze the online discourse between Kenyan internet users and government regulatory agencies and officials. To increase the transparency of the qualitative data analysis and to ensure the credibility of the research findings, the data from the social media platform and the in-depth interviews were subjected to Adu's, (2019) six steps of qualitative data analysis using

NVivo qualitative research software. Critical discourse analysis was used to analyse both the data from the Facebook social media platform and the in-depth interviews.

Findings and Discussion

Demographics

The study obtained 530 responses from the online survey of Kenyan Internet users. The majority of the study respondents were males with females comprising 38.5% (n = 204) of the study respondents. In terms of age, the majority were aged between 25-39 years comprising 43.6% (n = 231), the 18–24-year-olds accounted for 40.9 % (n = 217) and the 40–60-year-olds comprised 15.5% (n = 82). The study further sought to find out the education status of the respondents because their level of education would well determine how they responded to the questions that were asked. From the responses obtained, it was discovered that a majority of them, 76.8% (n = 407) had a degree level of education and above, 16.4% (n = 87) had a college diploma, 6.2% (n = 33) had attained the basic level of education and 0.6% (n = 3) did not attain any formal education.

The study also identified that the most popular social media platform among the participants was WhatsApp (31.2%%; n = 476) followed by Facebook (25.1%; n = 384), Twitter (18.4%, n = 281), Instagram (15.4% n=235) and others social network sites (9.9% n=138) in that order.

Threats for online safety on social media platforms

This study identified that vague and overbroad terminology used in some sections of the legislative Acts, human rights infringements, cyberbullying and the presence of illegal and harmful online content have been serious threats to online safety in Kenyan cyberspace.

Cyber-harassment

The findings revealed that cyberbullying and cyber harassment are among the online content threats that most Kenyans are exposed to and they dominated most of the online discourse on the Facebook social media platform. Local celebrities were not spared by the online cyberbullies and they have borne the brunt of most of the cyber-harassment on social media platforms. This was exemplified in the April 2020 incident when a local comedian, Mulamwah almost quit doing comedy due to being bullied on online platforms (Tuko Kenya, 2020). This scenario is further illustrated in the post below from an influential blogger;

> *Multitalented comedian Mulamwah has been forced to quit comedy after trolls overpowered him. He is always trolled on social media daily. (Post-ID 291, influential blogger).*

These findings echo the 2020 study of 171 countries by the United Nations Office on Drugs and Crime (UNODC) where they ranked Kenyans on the Twitter social media platform among the worst cyberbullies (Postamate, 2020). This is also consistent with the observations by Oluoch, (2019) and Wamuyu (2020) who noted earlier the inconvenience and psychological harm caused by harmful content and cyber threats on social media platforms.

Toxic online content

The study, for purposes of analysis grouped the online content that was both illegal and harmful as toxic online content. The findings identified that online discourse concerning illegal and harmful information dominated most of the conversations among Kenyans online. The findings indicated fake news, misinformation, and harmful content were largely discussed especially during the beginning of the COVID-19 pandemic. The posts below from some Facebook users identify the plight of internet users in dealing with toxic online content;

> *The growth of the internet and social networking platforms has elevated lies. And the more we use these platforms, the easier it is to spread fake news. (Post-ID 645 FB user).*
>
> *Celebs have been killed mercilessly by fake news blogs. (Post-ID 552 FB user).*

The influential bloggers have also through their Facebook social media pages engaged their followers in conversing about the increase of toxic content on the online platforms as reflected below.

> *Are you concerned about how toxic the internet has become? Fake news,*

> *misinformation, cyberbullying, revenge pornography, hate speech, and trolling. Are these topics of interest to you? Then #DoBetter and join the conversation let's talk. (Post-ID 350 influential blogger).*

The study findings also revealed that there were online conversations on how to handle harmful online content on online platforms, especially when it comes to protecting children online as illustrated in the word tree (Figure 1).

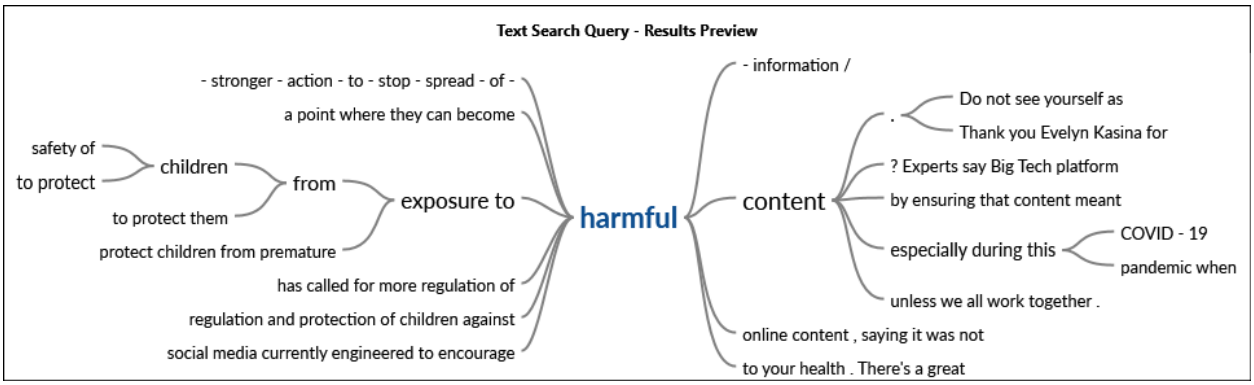

Figure 1. NVivo output: harmful word tree

Human rights infringements

The rights to Freedom of Expression, access to information, and privacy are very fundamental to the growth of democratic societies (Howie, 2018). In the Computer Misuse and Cybercrime Act (2018), some sections seem to infringe on the right to freedom of expression such as Sections 22 and 23 on false information. These sections have been challenged in court for being inconsistent with Article 33 of the Kenyan constitution (Sugow, 2019). Also, the right to privacy in Article 31 of the Kenyan constitution seems to be infringed by Section 51 of the Computer Misuse and Cybercrime Act 2018. This is because granting police officer's authority to issue a notice to a service provider for online traffic data on an individual without having to get approval from the court may make it prone to abuse. The fact that the section can be challenged in court negates its primary mandate for the effective preservation and disclosure of an individual's traffic data to aid an investigation into a cybercrime.

Court suspensions of Legislative Acts

The Computer Misuse and Cybercrime Act 2018 has severally been subjected to court cases challenging its constitutionality since it was accented in May 2018. As a result, this has led to the law being suspended on numerous occasions, therefore, limiting its implementation. In May 2018 the Bloggers Association of Kenya (BAKE) went to court to challenge the constitutionality of the Computer Misuse and Cybercrime Act 2018, stating that the Act infringed, threatened, and violated some of the fundamental freedoms in Chapter 4 of the Kenyan Constitution. The high court in its determination suspended 26 clauses of the Computer Misuse and Cybercrime Act 2018 for 21 months (*Petition 206 of 2018 Bloggers Association of Kenya (BAKE) v Attorney General & 5 others [2018]*).

Findings on the Facebook social media platform indicated differing perspectives of Kenyan users concerning cyberlaw, especially after the court's decision in February 2020 to dismiss the bloggers' petition (*Petition 206 of 2019 Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties) [2020]*). Some users who were not comfortable with the court's decision felt the need to appeal the High court's decision as shown in the posts below.

> *I'll challenge the Cybercrime law once the court resume. Sad that most sections that we challenged and won against have been returned through the backdoor. As I always say, No Quitting, we must fight for the upcoming bloggers because some of them*

> *may give up if fought like we are (Post-ID 428 influential blogger).*

However, in October 2020, 8 months into its being in effect after the earlier high court suspension, the Computer Misuse and Cybercrime Act 2018 was again suspended for another 9 months after the Senate went to court to challenge its constitutionality (Ogemba, 2020). In this case, the Senate moved to court to challenge the decisions of the National Assembly in passing legislation without their input. Consequently, this led to the suspensions by the High Court of 23 legislative Acts among them the Computer Misuse and Cybercrime Act 2018. (*Petition 284 & 353 of 2019 (Consolidated), Senate of the Republic of Kenya & 4 others v Speaker of the National Assembly & another; Attorney General & 7 others (Interested Parties) [2020] eKLR*).

Interventions to promote online safety

Findings from the study also noted that the Kenyan Government, Kenyan internet users including local celebrities as well as social media platforms have all been contributing towards advocating for online safety in Kenya's cyberspace.

Government interventions

The study findings identified some interventions that the Kenyan government has enacted and implemented such as coming up with specific laws such as the Computer Misuse and Cybercrime act 2018 and the Data Protection Act 2019 to govern cyberspace and promote online safety.

The judicial arm of the Government in Kenya has also played a key part in promoting online safety through its pronouncements on certain cases brought before the courts. The findings revealed that some Kenyan internet users appreciated the Court of Appeal's decision in the August 2020 ruling to dismiss the Law Society of Kenya (LSK) application for conservatory orders pending appeal from the judgment and orders of the High Court of Kenya given on 20th February 2020 in the High Court Petition No. 206 of 2018 which had earlier sought conservatory orders to suspend the coming into force of certain sections of the Computer Misuse and Cybercrimes Act 2018 (*Civil Application 102 of 2020. Law Society of Kenya v Bloggers Association of Kenya & 6 others [2020]).* These opinions were captured in the post below.

> *10 years in jail or 20 million fine if found guilty for #Cyberbullying rules Kenya court of appeal. This is such good news, especially after cases of online Violence increase. #stopcyberbullying (Post-ID 998 FB user).*

Moreover, the study findings also indicated that during the coronavirus pandemic, the government agencies were active and quick in refuting false information shared on social media platforms about them, their officers, actions, and processes (Figure 2).

Figure 2. Facebook posts (Post-ID 634 and 672 regulators Ministry of Interior)

Local celebrity's advocacy for clean content

This study identified that some online celebrities have advocated on their social media platforms the need for other users to embrace clean content in the online platforms. Some local music artists have also apologized to their fans for some of the illegal and harmful content they have shared on YouTube online platforms. This is exemplified by the Ethic Entertainment Music Group. The group faced a backlash from a section of Kenyans online when they released their song Tarimbo in 2019. '*Tarimbo*' which loosely translates to '*Crowbar*' was a 3-minute song laced with sexual innuendos with most Kenyans claiming it promotes rape culture (Kimuyu, 2019). The regulator, Kenya Film and Classification Board (KFCB) acted on the online music video as illustrated by the post below from the former KFCB CEO Dr. Ezekiel Mutua (Figure 3).

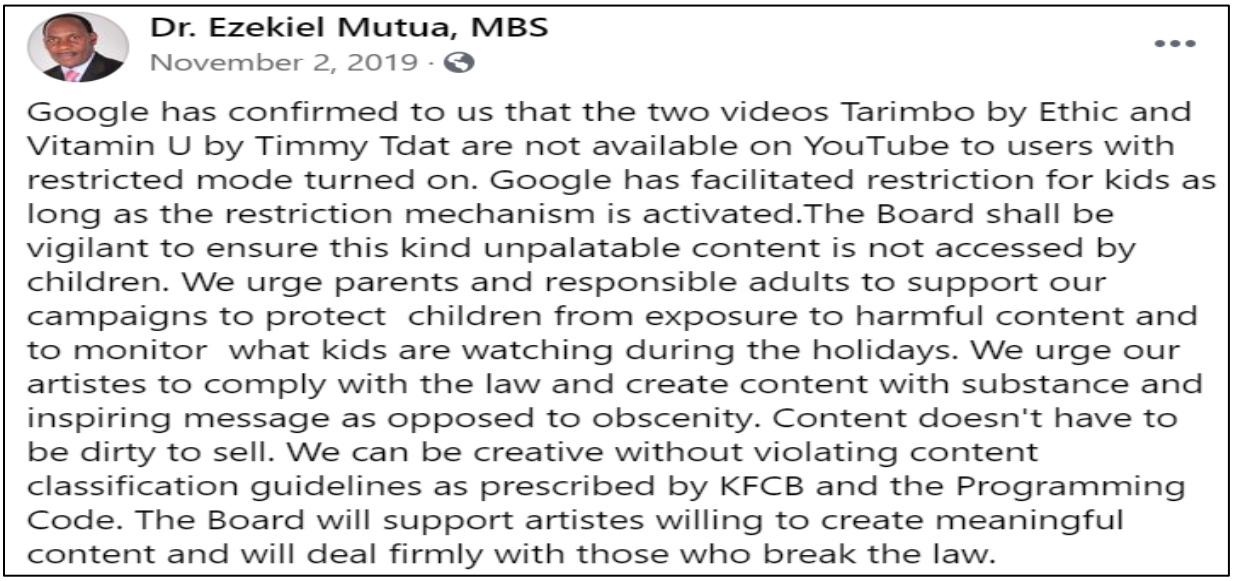

Figure 3. Facebook posts (Post-ID 810 regulator, Ezekiel Mutua)

In response, the Ethic Entertainment music group bowed to public pressure and promised to produce clean online music videos as shown by the post below from an influential blogger.

> *Ethic Entertainment music group has announced that it will be releasing a new and clean album on YouTube on June 13. This comes after their 'Tarimbo' song caused a public uproar in November 2019. The song was reportedly advocating for rape and promoting violence against women. The group apologized to their fans and promised to work and promote clean content. (Post-ID 24 influential blogger).*

Corporate players

The study findings indicated that in the wake of the coronavirus pandemic, several corporate organizations such as StarTimes, The United Nations Educational, Scientific and Cultural Organization (UNESCO), and the World Health Organization (WHO), joined efforts with the government authorities in promoting online safety on online platforms. This was done through online campaigns to dissuade people from illegal and harmful online content and irresponsible user behaviors as illustrated by the posts below.

> *StarTimes, UNESCO in a joint campaign against Dis- and Mis-Information on COVID-19 (Post-ID 559 Media hse).*

> *Kenya, UN to partner to promote girls' online safety (Post-ID 922 Media hse)*

Social media platforms have also been involved in conversations regarding online safety in Kenyan Cyberspace. Their participation and contribution to online safety are illustrated in the posts below from some of the internet users.

> *Facebook has rolled out a new campaign in East African countries including Kenya, Uganda, Tanzania, and Ethiopia to enlighten people on how to detect potential false news and ensure online safety. Now more than ever Facebook says that they are working to connect people to accurate sources, and show less misinformation, especially about COVID-19. Facebook has made significant investments to remove accounts and content that violates its policies (Post-ID 654 FB user)*

> *Good news! Twitter has also joined in the fight against fake news by providing new guidelines for Twitter users to be able to flag and counter fake information. #HowAfricaUpdates (Post-ID 636 FB user)*

As part of public appeals for online safety, this study revealed that the mainstream media has contributed to the discourse on online safety by advocating measures that they have put in place to counter false information in cyberspace. This is illustrated in the post below from one of the media houses.

> *Fake news is a major concern for us in the newsrooms and we have put in place measures to ensure that we don't fall for it ~ Mutuma Mathiu, Group Editorial Director, Nation Media Group (Post-ID 540 media hse).*

Public appeals for online safety

The study findings indicated that some Kenyans had also been encouraging online safety on online platforms by urging fellow users to beware and protect themselves from false information on the online platforms and verify their sources of information from credible sources such as the Ministry of Health. The content and context of these discussions are illustrated in the word tree (Figure 4).

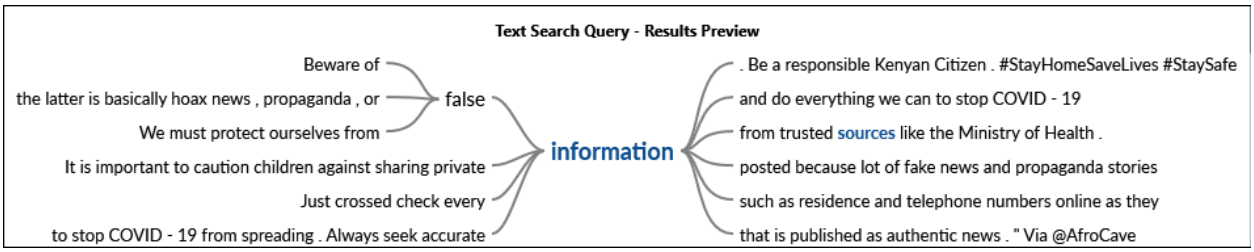

Figure 4. NVivo output: information Word tree

The need for child online safety was also advocated for in the online safety discourse on social media platforms. Some of the users urged parents to monitor what kids are accessing online as illustrated in the post below from one of the Facebook users;

> *We must talk to our children about online harassment by others or by the children to others. There is a need for parents to set family time and family rules on issues digital. #ChildOnlineSafety (Post-ID 972 FB user).*

In addressing the cyberbullying challenge, the study findings revealed that some of the users were advising fellow internet users to avoid cyberbullying as illustrated in the posts below from some of the Facebook users.

> *Let's make kindness online cool, no cyberbullying (Post-ID 299 FB user)*
>
> *Don't spread hate. (Post-ID 599 FB user)*

Internet users' online social responsibility

The study sought to examine whether there is a relationship between age and the extent that one would feel liable for the effects that emanate from the content that they post online. A Chi-square test of independence was performed and revealed that the relationship between the two variables was significant, X^2 (1, N = 530) = 53.023, $p < 0.001$. Those between the ages of 25-39 years indicated high levels of being liable for the effects that emanate from the content they posted online.

The study also examined the level of education *versus* the extent that one would feel responsible for the content that they posted online. A Chi-square test of independence was performed and it revealed that the relationship between these variables was significant, X^2 (1, N = 530) = 30.09, $p < 0.001$.

Influence of existing regulations on online safety

This study examined how Kenyan internet users perceived the effect of the existing online content regulations in promoting online safety in Kenyan cyberspace. This hypothesis was tested using regression model summary (R^2), inner loading (β), the p-value (one-tailed), and 95% bias-corrected confidence intervals. The hypothesis denoted as $\mathbf{H_1}$ (the existing content regulatory policies significantly affect online safety in Kenyan cyberspace) was accepted ($p = 0.000$; $R^2 = 0.785$) which means that 78.5% of the variation of online safety can be explained by the existing online content regulatory policies (Table 1).

Table 1. Results of regression model for hypothesis test (H_1) (a. Dependent Variable: Online Safety)

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.886[a]	.785	.785	.48331

a. Predictors: (Constant), Online Content Regulation

H_1 ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	450.897	1	450.897	1,930.330	.000[b]
	Residual	123.333	528	.234		
	Total	574.230	529			

a. Dependent Variable: Online Safety

b. Predictors: (Constant), Online Content Regulation

H_1 Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95.0% Confidence Interval for B	
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound
1	(Constant)	-.227	.067		-3.377	.001	-.359	-.095
	Online content Regulation	1.045	.024	.886	43.936	.000	.998	1.092

This study further examined whether Kenyan internet users' social responsibility moderated the effect of existing content regulatory policies in promoting online safety in Kenyan cyberspace. This hypothesis denoted as **H_2** (Social responsibility moderates the effect of existing content regulatory policies in promoting online safety in Kenyan cyberspace) was rejected (p = 0.461). This means, there is not enough evidence to support that social responsibility significantly moderates the effect of existing content regulatory policies in promoting online safety in Kenyan cyberspace (Table 2).

Table 2. Results of regression model for hypothesis test (H_2)

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.886[a]	.785	.785	.48352

a. Predictors: (Constant), Social responsibility, Online Content Regulation

H_2 ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	451.024	2	225.512	964.605	.000[b]
	Residual	123.206	527	.234		
	Total	574.230	529			

a. Dependent Variable: Online Safety

b. Predictors: (Constant), Social responsibility, Online Content Regulation

H_2 Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95.0% Confidence Interval for B	
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound
1	(Constant)	-.163	.110		-1.488	.137	-.379	.052
	Online content Regulation	1.044	.024	.885	43.813	.000	.997	1.091
	Social responsibility	-.016	.021	-.015	-.738	.461	-.058	.026

a. Dependent Variable: Online Safety

Additionally, this study examined whether the internet media environment significantly moderates internet users' perception of social responsibility in cyberspace (**H_3**). The results were statistically significant (p = 0.000; Table 3) and thus the hypothesis was accepted. The resultant $R^2 = 0.114$ suggests that 11.4% of the variation in the internet users' social responsibility can be explained by the internet media environment.

Table 3. Results of regression model for hypothesis test (H_3) (a. Dependent Variable: Social responsibility; b. Predictors: (Constant), Media Environment

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.337[a]	.114	.112	.92787

a. Predictors: (Constant), Media Environment

H_3 ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	58.216	1	58.216	67.619	.000[b]
	Residual	454.577	528	.861		
	Total	512.793	529			

H_3 Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95.0% Confidence Interval for B	
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound
1	(Constant)	2.900	.127		22.843	.000	2.650	3.149
	Media Environment	.310	.038	.337	8.223	.000	.236	.383

a. Dependent Variable: Social responsibility

It is clear that online content regulations play an important role in promoting online safety in cyberspace; however, regulations alone are insufficient to ensure a safe online environment. In dealing with the increasing cases of illegal online content in cyberspace, there is a greater need for collaboration between platform companies and governments. Collaborations between the industry, its citizens, and the government would respond to scholars' (Bada et al., 2019; Ogenga, 2019; Ryakitimbo, 2018) call for governments to use open and inclusive approaches in the development of online regulations.

However, while our findings show that internet users' social responsibility does not affect the effectiveness of existing online regulations in promoting online safety, the internet media environment, which is characterized by interactivity, significantly moderates internet users' perceptions of online social responsibility. This does support Cohen-Almagor's (2017) point about the importance of net citizens who are responsible and accountable for their actions in cyberspace. Responsible use of social media platforms is critical for furthering the discourse of online safety and upholding fundamental human rights. This is consistent with Waldron's, (2013) position on human dignity and human rights, which states that it is critical to associate the concept of human dignity with the responsibilities that each individual must accept for his or her own life (both online and offline) as well as Cohen-Almagor's, (2017) advocacy for net citizens. This is because net citizens contribute to the internet ecosystem's use and growth while attempting to ensure that their online content is constructive for the good of all humanity. Furthermore, internet users' online social responsibility would promote free speech, open access, and a social culture of respecting others and not harming others. As a result, the scope of illegal online content and irresponsible user behaviour will be reduced in the internet ecosystem.

Conclusion

The relationship between social media platforms, content regulation, and online safety will continue to grow as a result of the presence and influence of illegal online content. As a result, the importance of online safety in preventing online harm is critical. According to the findings of this study, more needs to be done to promote a safe, respectful, harmonious, and inclusive cyberspace. This is a global issue, not just one in Kenya. More internet users are needed to become net citizens, responsible and accountable for their actions and conduct in cyberspace.

Acknowledgments

I am grateful to Meta Inc. for assistance with granting me access to the Crowd-Tangle Platform, which enabled me to follow, analyse, and report on what was happening on the Facebook Social Media Platform at the time of conducting the research. I also have to express my appreciation to Professor Zhang Kai for sharing her pearls of wisdom during the course of this research.

References

Civil Application 102 of 2020. Law Society of Kenya v Bloggers Association of Kenya, Attorney General, National Assembly, Director of Public Prosecutions, Inspector General of Police, Article 19 East Africa & Kenya Union of Journalists [2020] eKLR http://kenyalaw.org/caselaw/cases/view/199748/

Petition 206 of 2018. Bloggers Association of Kenya (BAKE) v Attorney General, Speaker, National Assembly, Inspector General of the National Police Service & Director of Public Prosecutions; Article 19 East Africa & Kenya Union of Journalists (Interested Parties) [2018] eKLR http://kenyalaw.org/caselaw/cases/view/159286

Petition 206 of 2019. Bloggers Association of Kenya (BAKE) v Attorney General, Speaker, National Assembly, Inspector General of the National Police Service & Director of Public Prosecutions; Article 19 East Africa & Kenya Union of Journalists (Interested Parties) [2020] eKLR. http://kenyalaw.org/caselaw/cases/view/191276/

Petition 284 & 353 of 2019 (Consolidated), Senate of the Republic of Kenya, Speaker of the Senate, Senate Majority Leader, Senate Minority Leader & Council of County Governors v Speaker of the National Assembly & National Assembly of Kenya; Attorney General, Kenya Medical Supplies Authority, Institute for Social Accountability, Mission for Essential Drugs & Supplies, Katiba Institute, Pharmaceutical Society of Kenya, Elias Murundu & Commission on Revenue Allocation(Interested Parties) [2020] eKLR).

http://kenyalaw.org/caselaw/cases/view/202549/

Adonijah O. (2019). "Focus on awareness as Kenya's cyber threats jump to 135pc" *Africa Sustainability Matters,* October 1. https://africasustainabilitymatters.com/focus-on-awareness-as-kenyas-cyber-threats-jump-135pc/

Adu, P. (2019). *A step-by-step guide to qualitative data coding*. Routledge, United Kingdom, 288, ISBN: 978-1138486874.

Bada, M., Von Solms, B., & Agrafiotis, I. (2018). "Reviewing National Cybersecurity Awareness in Africa: An Empirical Study." In *Thinkmind Digital Library*. https://www.repository.cam.ac.uk/bitstream/handle/1810/293742/Bada.et.al.pdf?sequence=3

Barker, K. & Jurasz, O. (2019). "Online Harms White Paper Consultation Response". *Striling Law School & the Open University Law School.* http://oro.open.ac.uk/69840/1/Barker%20%26%20Jurasz%20%20Online%20Harms%20White%20Paper%20Consultation%20Response%20%282019%29%20.pdf

Barnard, J. S. (2016). "A Brave New Borderless World: Standardization Would End Decades of Inconsistency in Determining Proper Personal Jurisdiction on Cyberspace Cases". *Seattle University Law Review.* 40:249. https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=2367&context=sulr

Cable.Co.Uk. (2021). "Worldwide Broadband Speed League 2021 | Internet Speed Tests". Cable.Co.Uk. Accessed November 13, 2021. https://www.cable.co.uk/broadband/speed/worldwide-speed-league/

Cohen-Almagor, R. (2017). Balancing freedom of expression and social responsibility on the internet. *Philosophia*. 45(3): 973-985. https://doi.org/10.1007/s11406-017-9856-6

De Kimpe, L., Walrave, M., Ponnet, K. & van Ouytsel, J. (2019). Internet safety. *The International Encyclopedia of Media Literacy*. 1-11. DOI: 10.1002/9781118978238.ieml0093

Facebook. (2017). Community Standards. https://en-gb.facebook.com/communitystandards.

Howie, E. (2018). Protecting the human right to freedom of expression in international law. *International Journal of Speech-language Pathology*, 20(1):12-15 DOI:10.1080/17549507.2018.1392612

Kimuyu, H. (2019). "Ethic's halfhearted apology for Tarimbo". *Nairobi News.* November 5. https://nairobinews.nation.co.ke/chillax/ethics-halfhearted-apology-for-tarimbo

Macaulay, P. J., Boulton, M. J., Betts, L. R., Boulton, L., Camerone, E., Down, J. & Kirkham, R. (2020). Subjective *versus* objective knowledge of online safety/dangers as predictors of children's perceived online safety and attitudes towards e-safety education in the United Kingdom. *Journal of Children and Media*. 14(3): 376-395. DOI:10.1080/17482798.2019.1697716

Mazur, E., Margaret, L.& Michelle, H. (2019). The internet behavior of older adults. Chap 32. In *Advanced Methodologies and Technologies in Media and Communications*. IGI Global. DOI: 10.4018/978-1-5225-7601-3.ch032

Ministry of Devolution and Planning. (2013). Second Medium-Term Plan (2013-2017) Kenya Vision 2030. In Vision2030.go.ke. https://vision2030.go.ke/2013-2017/

Odgers, C. L., Stephen, M. S., & Mimi, I. (2020). Screen Time, Social Media Use, and Adolescent Development. *Annual Review of Developmental Psychology*. 2:485-502. https://doi.org/10.1146/annurev-devpsych-121318-084815

Ogemba, P. (2020). "Win for Senate in supremacy war as court declares 23 laws unconstitutional". *Standard Media Group*.

https://www.standardmedia.co.ke/nairobi/article/2001391976/judges-strike-out-23-laws-that-mps-passed-illegally

Ogenga, F. (2019). *Peace Journalism in East Africa: A Manual for Media Practitioners*. Routledge Routledge, Taylor & Francis Group.

Oluoch, V. (2019). "Shortage of skilled cybersecurity experts exposes ICT sector to". *Daily Nation,* May 26. https://nation.africa/kenya/newsplex/shortage-of-skilled-cybersecurity-experts-exposes-ict-sector-to-huge-losses-171136

Pinter, A. T., Pamela, J. W., Heng, X., Mary B. R., & Jack, M. C. (2017). Adolescent online safety: Moving beyond formative evaluations to designing solutions for the future. *In Proceedings of the 2017 Conference on Interaction Design and Children*. 352-357. https://dl.acm.org/doi/pdf/10.1145/3078072.3079722

Plaisance, P. L. (2013). "Media ethics." *International Encyclopedia of Ethics*. 1-11. Accessed October 13, 2021. http://cognella-titles-sneakpreviews.s3.amazonaws.com/82974-1A-URT/82974-1A_SP.pdf

Postamate, (Ed) (2020). "Kenyans Ranked as the Worst Bullies on Twitter by UN body". *Postamate website*. April 15. Accessed October 13, 2021. https://postamate.com/2020/04/kenyans-ranked-as-the-worst-bullies-on-twitter-by-un-body/

Ryakitimbo, R. (2018). "Fake news and vague laws: Online content regulation in Africa". *African School on Internet Governance website* November 28. https://afrisig.org/2018/11/28/fake-news-and-vague-laws-online-content-regulation-in-africa/

Siebert, F., Fred, T. S., Theodore, P., Theodore, B. P., & Wilbur, S. (1956). *Four theories of the press: Authoritarian, libertarian, social responsibility, and soviet communist concepts of what the press should be and do*. Vol. 10. University of Illinois Press.

Stork, C. & Esselaar, S. (2019). "When the People Talk: Understanding the Impact of Taxation in the ICT sector in Benin". Washington DC: Alliance for Affordable Internet. https://1e8q3q16vyc81g8l3h3md6q5f5e-wpengine.netdna-ssl.com/wp-content/uploads/2019/03/A4AI_Benin-Tax-Report_Screen_AW.pdf

Sugow, A. (2019). The Right to be Wrong: Examining the (Im) possibilities of Regulating Fake News while Preserving the Freedom of Expression in Kenya. *Strathmore Law Review.* 4:19. https://press.strathmore.edu/uploads/journals/strathmore-law-review/SLR4/The%20Right%20to%20be%20Wrong.pdf

Tambini, D. (2019). The differentiated duty of care: a response to the Online Harms White Paper. *Journal of Media Law*, *11*(1), 28-40. DOI: 10.1080/17577632.2019.1666488

Tsai, Hsin-Yi Sandy, Mengtian Jiang, Saleem Alhabash, Robert LaRose, Nora J. Rifon, and Shelia R. Cotten. (2016). "Understanding online safety behaviors: A protection motivation theory perspective." *Computers & Security* 59: 138-150. https://doi.org/10.1016/j.cose.2016.02.009

Tuko Kenya. (2020). "Mulamwah quits comedy over Cyberbullying by Kenyans on Twitter". Tuko *Television*, April 14. https://www.youtube.com/watch?v=CRYOASfuRX8

Twitter Help Center. (2019). "The Twitter Rules". *Twitter.com website* February 12. https://help.twitter.com/en/rules-and-policies/twitter-rules

Vraga, E. K., Melissa, T., & Leticia, B. (2020). Empowering users to respond to misinformation about COVID-19. *Media and Communication, 8*(2), 475-479.

https://doi.org/10.17645/mac.v8i2.3200

Wainaina, W. (2019). "Surge in cyberattacks presents new opportunities for insurers". *Standard Media Group* September 10. https://www.standardmedia.co.ke/business/article/2001341416/surge-in-cyber-attacks-presents-new-opportunities-for-insurers

Waldron, J. (2013). "Is dignity the foundation of human rights?" *NYU School of Law, Public Law* Research Paper 12-73. https://web.archive.org/web/20160914024954id_/http://lsr.nellco.org:80/cgi/viewcontent.cgi?article=1376&context=nyu_plltwp

Wamuyu, P. K. (2020). "The Kenyan Social Media Landscape: Trends and Emerging Narratives". 2020. Accessed November 13, 2021. https://usiu.ac.ke/assets/image/Kenya_Social_Media_Lanscape_Report_2020.pdf

Wright, J., & Javid, S. (2019). *Online harms White Paper*, Department for Digital, Culture, Media, and Sport. https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper

World Economic Forum. (2019). "The Global Risks Report 2019 14th Edition Insight Report". http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Wisniewski, P. (2018). The privacy paradox of adolescent online safety: A matter of risk prevention or risk resilience? *IEEE Security and Privacy 16*(2), 86-90. DOI:10.1109/MSP.2018.1870874

Yar, M. (2018). "A failure to regulate? The demands and dilemmas of tackling illegal content and behaviour on social media." *International Journal of Cybersecurity Intelligence & Cybercrime 1*(1), 5-20. https://www.doi.org/10.52306/01010318RVZE9940

You, Y., & Zhengxu W. (2020). The Internet, political trust, and regime types: A cross-national and multilevel analysis. *Japanese Journal of Political Science*, *21*(2), 68-89. doi:10.1017/S1468109919000203