The dark side of social media in Zimbabwe: Unpacking the legal framework conundrum

Ishmael Mugari

Abstract: Despite their numerous benefits to humanity, social media platforms have brought new challenges on the national security landscape. Irresponsible use of social media has resulted in social vices such as violence, terrorism, child pornography and a myriad of other social ills. To counter the social media-induced threats, most nations have resorted to strict regulatory frameworks that criminalise and penalise some of the social media actions that are viewed as threats to national security. This paper, which is largely based on a literature and documentary survey, explores the threats posed by social media in Zimbabwe. The paper also evaluates the regulatory framework for control of the social media threats in Zimbabwe. The paper reveals that social media platforms have been used to instigate violent protests, to issue subversive statements and to spread fake news, causing fear and despondency amongst citizens. Social media platforms have also been used to facilitate other crimes such as human trafficking and distribution of pornographic material. While several existing statutes have been invoked in the face of these threats, the absence of a specific law to deal with social media threats militates against the current legal framework.

Subjects: Information & Communication Technology; ICT; Criminology - Law; Communication Ethics; Information Technology

Key words: Social media; national security; social movement; violence; constitution; regulation

ABOUT THE AUTHOR

Ishmael Mugari holds a doctorate in policing and is a lecturer in the Department of Intelligence and Security Studies at Bindura University of Science Education in the Republic of Zimbabwe. His research focuses on criminology, police accountability, police strategy and national security issues. This article focuses on the impact of technology, specifically social media, on national security. It also exposes the limitations of the legislative framework in policing social media threats to national security.

PUBLIC INTEREST STATEMENT

This paper explores the threats that are posed by social media in Zimbabwe, a developing country that has been characterised by an upswing in social media usage amidst socio-economic challenges. The paper reveals that social media platforms have been used to foment violent protests, spread fake news intended to cause panic and political intrigue, and to facilitate crimes such as human trafficking and distribution of pornographic material. The paper also reveals the limitations of the current legal framework to address social media threats to national security, as well as providing an argument for speedy promulgation of a comprehensive piece of legislation that addresses social media threats to national security.
1. Introduction

The advancement in technology across the globe has revolutionised the way in which people interact. The advent of social media, a manifestation of advancement in technology, has heavily impacted on communication. Whether in relation to social networking (Facebook), photo and video sharing (Instagram, YouTube), or micro-blogging (Twitter) sites, social media have transformed media systems, irrevocably altering dynamics of production, consumption, and dissemination (Walsh & O’Connor, 2019). Social media have also challenged information hierarchies, opened up access and produced an entirely new ecosystem of information exchange (Pandalai, 2016). In contrast with traditional media, social media are distributed and participatory systems of communication where those formerly known as audience emerge as producers of large quantities of “user generated content” (Walsh & O’Connor, 2019). Thus, citizens are now empowered as subjects of communication and are empowered to directly shape public discourse and opinion. Social media allow people around the globe to connect and share information in real-time, thus bringing convenience. Moreover, users can follow or be followed by others, arrangements that facilitate the instantaneous dissemination of content and display “viral” qualities, where information can rapidly, and often unpredictably, cascade across networks (Yar, 2014). Another important feature of social media is their symbiotic relationship with traditional media (mainly television), where traditional media are increasingly relying on social media to feed their 24-h news cycles, as well as covering stories that emanate from social media platforms.

Notwithstanding their growing impact and reach, as well as their ability to shape public discourse and opinions, social media present real opportunities. In the political circles, social media have been used as communication platforms to enhance participative democracy (Klang, 2011; Pandalai, 2016). In this regard, social media have opened new avenues for civic participation in political processes, inspiring hopes for a democratic reinvigoration (Bradshaw & Howard, 2018). During times of disasters, social media platforms have been used as vital tools for conveying information on disaster awareness and management (Bruce, 2011; Klang, 2011; Lumpp, 2014). For example, during and in the aftermath of Hurricane Sandy in 2012, which shattered a large part of the New York City metropolitan area, the Federal Emergency Management Agency (FEMA) used social media to disseminate information about the storm before it struck, locations that had power to charge cell phones, locations where citizens could take shelter, get water and food, and other aid available in the area (Lumpp, 2014). Similarly, during the Haiti earthquake, social media enabled citizens’ engagement through supporting the dissemination of information on evacuation and rescue experiences, as well as sending of alert messages (Hodge, 2010).

Perhaps the most potent use of social media, with a direct bearing on national security, is their importance in the policing discourse. Social media platforms have been used as open-source intelligence platforms (Fitsanakis & Bolden, 2012). Given that social media enable the police to access private information with little effort (Trottier, 2012), police in several countries have harnessed social media’s potential through deploying intelligence units to conduct online surveillance, reconstruct events, and extract official knowledge about the activities, personalities, and motivations of suspects (Walsh & O’Connor, 2019). Twitter can be used to circulate real-time alerts about risk and crime-related events (Walsh, 2019), as well as to build trust and support through posting messages about successful enforcement (Schneider, 2016). Social media platforms have also been used to combat civil unrest, as well as to combat terrorism (AlZaabi & Tomic, 2018; Kimutai, 2014). For instance, after the 2011 Vancouver Stanley Cup riots, authorities utilised facial recognition software to scrutinise photos and videos published on Facebook by participants, bystanders, and outraged citizens seeking to “name and shame” alleged rioters-efforts that facilitated hundreds of arrests (Trottier, 2012). Similarly, during the Boston Marathon bombings, local and federal law enforcement officials monitored content posted on Reddit, Facebook, Twitter, and YouTube to help identify the perpetrators (Walsh & O’Connor, 2019), and used Twitter to keep the public informed about the status of the probe, to calm nerves and request public assistance, and to correct misinformation by the press (Pandalai, 2016; Edwards et al, 2014).
Despite their positive implications on humanity, social media platforms portend a double-edged sword, as they have posed new challenges in the realm of personal and national security. On a personal level, Rose (2011) warns that there are greater chances of private information becoming public, which opens users to various security risks as the information is easily transferred between social media platforms. Over-sharing of information on social media networks also increases vulnerability of location-based information, thus posing a threat to citizens’ privacy (Rose, 2011). The threats to privacy are compounded by the fact that social media platforms are relatively easy to access, and posted content can be easily seen and reviewed by anyone with an interest in the user’s personal information.

There is much documented evidence of the impact of social media on the broad national security discourse in both the developed and developing world. Terrorism, one of the leading threats to global security, has been propagated by social media platforms. Terrorist organisations such as al Qaeda and the Islamic State of Iraq and Syria (ISIS) have been using social media to recruit (Kimutai, 2014; Liaropoulos, 2013; Pandalai, 2016) and to radicalise citizens (AlZaabi & Tomic, 2018). Specifically, ISIS has been using social media platforms such as Twitter, Facebook, YouTube, WhatsApp and Skype to lure mostly Western recruits to Syria for terrorist training (AlZaabi & Tomic, 2018). Terrorists are using social media platforms to announce their successful attacks, thereby causing fear and panic amongst citizens (Borau & Wambé, 2019). The problem is compounded by the fact that once they publish their successful attacks on social media platforms, this will create a permanent online record. Similarly, social media platforms have also been used to facilitate violent protests. For instance, during the 2011 England riots, teenage gangs used social media communication platforms to evade authorities, publicise lawlessness and coordinate anti-social behaviour (Fuchs, 2013).

In some parts of the world, social media platforms have been used as powerful communication tools for fuelling social and political upheaval. Through social media platforms, activists are able to overcome censorship, coordinate protests, and spread rumour with ease in instances where regimes stifle dissent and try to control public discourse (Tufekci, 2017). Protests in Tunisia and Egypt, which led to an overthrow of sitting presidents, were coordinated through social media. Summarising the impact of social media in the Tunisia and Egypt revolutions, Liaropoulos (2013) highlighted that social media managed to spread the message in the early phase, mobilised part of the local population, and drew international attention. In his analysis of the Arab Spring revolution, Cuman (2012) also concurred that the usage and growth of social media in the Arab region played a significant role in mass mobilisation of protestors, empowerment, shaping of opinions and influencing change.

Social media platforms have also been instrumental in the spread of fake news, with the intent to cause fear and panic among citizens (Bradshaw & Howard, 2018; Walsh, 2020). Fake news, defined as news which is wholly false or containing deliberately misleading elements incorporated within its content (Bakir & McStay, 2018), is widely circulated online. Fake news that is propagated through social media platforms can also have implications on the economic well being of a nation. For example, in 2013, the Associated Press’s Twitter account was hacked and released a tweet falsely claiming that there had been two explosions at the White House and that President Obama had been injured (Forster, 2013). Within 2 minutes, the tweet had reached US stock traders and the Dow Jones dropped over 143 points (a $136.5 billion loss). Although the tweet was discovered to be erroneous and taken down within minutes, the damage had been done and this was a wakeup call for security analysts and policymakers to consider the negative implications of believing false information (Forster, 2013). The manipulation of public opinion over social media platforms has also emerged as a critical threat to public life (Walsh, 2020) and this phenomenon has been rife during political campaigns in different countries (Bradshaw & Howard, 2018). In their report on social media manipulation during political campaigns, Bradshaw and Howard (2018) found out that there were organised social media manipulation campaigns, which were characterised by misinformation, in 48 countries. There have also been fears that fake news may have influenced
the 2016 United States presidential election’s outcome (Bakir & McStay, 2018). For instance, the most engaged-with, yet fake story, was the story which claimed that Pope Francis had endorsed Donald Trump for President and the story amassed 960 000 shares on Facebook (Price, 2016 in Bakir & McStay, 2018).

In his study on social media and moral panic, Walsh (2020) contends that social media favour content likely to generate significant emotion and outrage, thus making it a facilitator of division and hostility. Such content’s emotional valence infects other users, influencing their subsequent interactions and escalating bitterness within online environments (Walsh, 2020). Such social media-induced hostilities were witnessed during the xenophobic attacks in South Africa in 2015 and 2019, which were perpetrated by South African citizens on foreign nationals—mainly Zimbabweans, whom South Africans accused of taking their job opportunities and committing criminal activities. Social media platforms played a significant role in perpetuating the xenophobic attacks, which were characterised by beating and sometimes killing of foreigners, as well as looting of foreigners’ shops. The Citizen Research Centre [CRC] (2019) noted that during the 2015 xenophobic attacks, a total of 21 660 social media posts were classified as either extreme hate speech or an incitement to violence. The study by CRC also noted the influence of social media in broadcasting irresponsible xenophobic statements by key political figures, with some of the reckless statements triggering the xenophobic attacks (Citizen Research Centre [CRC], 2019). News24 (2019) also noted the impact of misleading social media posts as a precursor to some of the xenophobic attacks in 2019. Social media was awash with old videos purporting to be current xenophobic attacks, with some of the videos not originating from South Africa (News24, 2019).

Thus, in the context of South Africa, social media was used to instigate violence in two ways: first, through inciting citizens to act against foreigners, and second, through spreading false information pertaining to alleged xenophobic attacks.

1.1. Theoretical framework

Several theories have been propounded to help in understanding the threat posed by social media to the socio-economic wellbeing of citizens, in general, and the national security, in particular. This paper was mainly informed by two sociological theories, namely; the social movement theory and the social responsibility theory.

1.1.1. The social movement theory

The social movement theory provides a context to the impact of social media on national security by explaining the dynamics of unrest and protest movements. According to Ghanim (2012), social movements can be viewed as collective enterprises to establish a new order of life, whose motive is two pronged; first, they are dissatisfied with the current form of life, and second, they have hope for a new system of living. Thus, the social movement theory best explains political struggles that eventuate into violent protests. Tilly (2011) points out that political struggle can take place through protests and collective action. Protests are generally an expression of popular consciousness that is manifested in street politics, while collective action occurs when a population has a shared interest and coordinates action on behalf of that interest (Kimutai, 2014). The theory also posits that collective action is more likely to bear fruit in communities with strong network ties. Those who share the same interests and ties with the majority in the movement will be easily recruited into the movement. The group will mainly be composed of individuals who share common interests, attributes, activities and causes.

The social movement theory vividly explains the role that social media platforms can play during political upheavals and other protest action. Through various social media platforms, the capacity and speed of establishing and maintaining social networks for a political objective will be improved. Movements can use social media platforms to further their goals, as these technologies allow people to find one another, to craft and amplify their own narrative, to reach out to broader publics, and to organize and resist (Tufekci, 2017). Thus, the ability to use digital tools such as social media platforms to rapidly amass large numbers of protesters with a common goal
empowers movements (Tufekci, 2017). For instance, during the 2011 uprising in Egypt, a popular Facebook page, created to decry the beating to death of a young man by the Egyptian police, became the forum for organizing the initial Tahrir uprising and had mustered hundreds of thousands of supporters (Tufekci, 2017). In nations where the democratic space is stifled, and where it is difficult to establish formal structures to confront the regimes, social media platforms are used to organise protests in the absence of formal structures. These platforms, as Tufekci (2017) argues, portend new capabilities for protestors to reimagine and alter the practice of protests and movement building. Moreover, in a highly polarised and repressive political environment, social media can also facilitate platforms for expression, thus reducing some of the risks of public activism (Kimutai, 2014). Importantly, once a clear political drive has been established, Walsh and O’Connor (2019) note that social media can help promote and coordinate offline resistance and activism through publicising demonstrations and encouraging participation.

1.1.2. The social responsibility theory
The social responsibility theory provides for a responsible use of all media platforms. According to Philip (2001), the social responsibility theory postulates that the media ought to serve the public, and in order to do so, should remain independent of government interference. Social media platforms contribute to the development of a “monitory democracy”, allowing citizens to directly act as watchdogs and ombudsmen, rather than relying on journalists and other mediating institutions (Walsh & O’Connor, 2019). In relation to police accountability, social media use is predominantly oriented towards educating the citizens about police brutality, structural racism, the amplification of marginalised voices, and police reform (Freelon et al, 2016, in Walsh & O’Connor, 2019). To this end, the visibility of social media will promote accountability, unmask corruption and abuse of power, and encourage awareness and action. Whilst social media provide citizens with alternative information, especially where traditional media channels are controlled by the state, the social responsibility theory requires that social media should report accurately and responsibly. This, however, has not been the case, as empirical research (Bakir & McStay, 2018; Bradshaw & Howard, 2018; Walsh, 2020) has shown the social media platforms’ propensity to spread fake news and to cause moral panic.

Underpinned by the need for responsible news reporting, there is a need for governments to guard against the irresponsible use of social media. In order to safeguard media independence, the government should, however, only set the parameters within which the media should operate in order to achieve its objective. A key phenomenon of this theory as opined by Philip (2001) is that the media should be self-regulating through devotion to diverse precepts such as the obligation to preserve freedom, high principles of objectivity and professionalism, truth and accuracy, and at the same time reflecting the diversity of the cultures represented. In practice, nonetheless, the social responsibility theory is complex to fulfil as regimes the world over-regulate the operations of the media, thus curtailing the operations of the media. Political hegemonies the world over, whilst arguing that security is essential for their countries’ defence, development and political survival, craft various legislative pieces, debatably, to stifle the media. Moreover, several democracies have established new government agencies or mandated existing organisations to combat fake news (Bradshaw & Howard, 2018). It is also this concept of the desire to have socially responsible citizens, who are self-regulating and who abide by the state’s legislative requirements, which also informed this study.

1.2. Social media in the Zimbabwean context
Despite being a developing country, Zimbabwe has followed the global trend of embracing social media as key communication platforms. There has been an upswing in the use of social media in Zimbabwe, with social media platforms dominated by WhatsApp, Facebook and Twitter, amongst other social media platforms. The Media Institute of Southern Africa (MISA) (2018) notes that mobile internet makes up for most of the internet accessed in the country, with the bulk of its use being on social media applications. WhatsApp is predominantly used and in 2017, 47% of the total data bundles purchased were for WhatsApp (Media Institute of Southern Africa (MISA), 2018). The increase in social media usage could be attributed to a rise in mobile telecommunication
subscribers, with Media Institute of Southern Africa (MISA) (2018) reporting that the mobile subscriber base rose from 11.4 million in 2014 to 14 million in 2017.

Similarly, a poll by the Voice of Zimbabwe in 2018 established a phenomenal rise in the use of social media as news platforms, with 52.3% of Zimbabweans getting their news from WhatsApp, Twitter and Facebook (Sengere, 2018). The same study established that 32.5% of Zimbabweans think that social media is a reliable source of news (Sengere, 2018). Consequently, Zimbabwean mainstream media- the newspaper, radio and television, have been outpaced by social media (Nyoni, 2017). The polarised mainstream media, which is characterised by a single state-owned television station and several state-owned radio stations (Nyoni, 2017), makes social media platforms indispensable alternative sources of information for Zimbabwean citizens.

Whilst the government can tap into the numerous benefits of social media, the upswing in the use of social media platforms also comes at a cost. The government and its various institutions have, on numerous occasions, had to contend with the threats posed by social media. This paper explores the threats that the social media pose onto the national security of Zimbabwe. In the face of the social media-induced threats, one of the measures to deal with the threats is the regulatory framework. Though several measures are available to deal with social media-induced threats to national security, this paper evaluates the current legal framework for regulating social media operations in Zimbabwe. The paper provides context-specific information on an emerging threat to national security for a developing country. Whilst several studies have been conducted on the threat of social media in other countries across the globe, there is limited focused empirical research on this contemporary threat in Zimbabwe.

2. Methodology
This exploratory paper was based on an internet search of articles and documents on the threats posed by social media in Zimbabwe. In this regard, this exploratory paper synthesised sparse literature and documentary evidence of the threats that social media pose on Zimbabwe's national security. An internet search was conducted on Google Chrome using key search words, “Social media and national security in Zimbabwe; social media threats in Zimbabwe; social media regulation in Zimbabwe”. The articles and documents that were reviewed spanned from 2013 to 2020. This period was considered for two reasons: First, from the year 2013, Zimbabwe began to witness a phenomenal rise in mobile telecommunication subscribers, which in turn resulted in the rise in social media platforms use (Media Institute of Southern Africa (MISA), 2018); and second, most notable social media threats to national security began to be witnessed in the run up to the 2013 general elections. A total of 22 relevant articles and documents were identified after an internet search and these included research articles (n=2), online news articles from the state media (n=5), online news articles from independent media (n=12), documents that were written by human rights-based non-governmental organisations (n=2), and a report from a commission of inquiry (n=1). A fusion of articles from the state media channels and independent media channels necessitated a balanced analysis of the social media threats to national security in Zimbabwe. Moreover, of the 12 independent media channels, two articles were from United States media outlets- The Business Insider and the Washington Post, thus necessitating an independent external assessment. Importantly, the researcher also examined some of the social media messages (mainly WatsApp and Facebook) that were deemed to be either fake or inflammatory.

Given that this paper only looked at the regulatory framework as a response to social media-induced threats to national security, the researcher evaluated the current laws that have been invoked to deal with social media-induced threats to national security. First, the relevant constitutional provisions were reviewed, in addition to the following Acts: Postal and Telecommunications Act [Chapter 12:05] of 2000; Official Secrets Act [Chapter 11:09] of 2001; Access to Information
and Protection of Privacy Act [Chapter 10:27] of 2002; Criminal Law [Codification and Reform] Act [Chapter 9:23] of 2004; and the Interception of Communications Act [Chapter 11:20] of 2007.

Whilst the absence of primary data through questionnaires and interviews may be the major limitation, this exploratory paper provides a vivid picture on the real threats that the social media platforms are posing to Zimbabwe’s national security, as well as how the existing legal framework is faring in dealing with these real threats. Moreover, despite vast research on the social media threats to national security in the developed world, there has been limited empirical research for developing countries in general, and for Zimbabwe, in particular. This study will provide an impetus for future researchers to look at social media implications on national security in the developing world.

3. Findings and discussion

3.1. Social media threats to national security in Zimbabwe

Despite the limited empirical research on the threats posed by social media in Zimbabwe, documentary evidence is available in various media platforms. Perhaps the first significant case on the impact of social media on national security is that of a Facebook character known as Baba Jukwa (loosely translated to Father of Jukwa), who rose to prominence in the run up to the 2013 harmonised elections in Zimbabwe. Baba Jukwa was a “faceless” Facebook character, who became popular for exposing corruption, plots and “murders” in Zimbabwean politics, and other tabooed subjects (Mujere & Mwatwa, 2015). Every day, the account published tales of corruption and brutality, often leaving the phone numbers of implicated politicians, so that readers could call them (Taylor, 2013). At one time, the Facebook character posted a message threatening to abduct the children of a serving cabinet minister, after accusing the minister of causing the death of a prominent politician. He indicated that it was time for violence, and remarked, “it is now fire with fire, blood with blood” (Taylor, 2013). Another threat, which sent the security institutions and the citizens into shock, emanated from a post which indicated that a reserve army, which was named the Zimbabwe Revolutionary Army, had been put in place to overthrow the government. The page also contained some posts which reportedly encouraged rebellion against the government if the 2013 general elections were stolen (Charles, 2014). Given that the Facebook page had half a million followers by 2014 (Taylor, 2014), the page had significant implications on the political environment and the national security of Zimbabwe. The Facebook posts caused fear, panic and despondency among the politicians and the citizens. This was a major wakeup call for the government and its security apparatus to seriously consider the threat that social media poses on national security and governance. In a rather puzzling development, an editor of a leading government-owned weekly newspaper- The Sunday Mail, was arrested after it was alleged that he was the brains behind the Baba Jukwa page (Charles, 2014). Several other suspects, amongst them journalists, were also arrested and two high profile ruling party politicians were also invited for questioning by the police. Surprising though, posting on the page stopped when the suspects were arrested, though up to date, neither a conviction has been secured, nor has the puzzle as to who Baba Jukwa was, has been solved.

In 2016, Zimbabwe had to contend with another social media-induced threat to national security in the form of violent protests. The protests were sparked by a video that was released by a cleric- Evan Mawarire, through his Facebook page and YouTube, in which he criticised the government for bad governance while wearing a Zimbabwean flag around his neck (News24, 2019). The video was part of a campaign entitled #ThisFlag and #ShutdownZimbabwe, which encouraged citizens to strike and stay at home in order to induce the government to address socio-economic challenges. Notwithstanding the movement’s justification for their actions, namely to implore the government to address economic and governance issues, their social media actions sparked widespread protests throughout 2016. The protestors were calling for resignation of the then President Mugabe, whom they accused of economic mismanagement and human rights violations. Despite the fact that protests are a constitutional right, the protests were deemed to
be illegal by the Zimbabwean police. It can be argued that the attempt by the police to thwart the protests may have escalated the violence, especially given the fact that citizens had held peaceful protests before. Notwithstanding the need for the authorities to uphold the citizens’ right to protest, resorting to violence, by both the protesting citizens and the state security authorities, also constitutes violation of other citizens’ rights.

The social media-induced violent protests seem to mirror the Arab Spring Uprising (Cuman, 2012; Liaropoulos, 2013) where social media platforms were used to incite citizens to revolt against the government, albeit with a different result. The 2016 violent protests in Zimbabwe could have been a build up to a mega protest in 2017, where citizens were protesting against the then President Robert Mugabe. The protest, coupled with a military-assisted transition, led to the resignation of the then President. The politically motivated violent protests and the change of government in 2017 attest to the relevance of the social movement theory, in which citizens can gather through social media to express their anger or opinion, leading to a political change.

Social media took centre stage during the disputed July 2018 harmonised elections. Violent protests broke out on the 1st of August 2018, with protestors demanding the announcement of presidential results by the Zimbabwe Electoral Commission. In its findings, The Commission of Enquiry on the August 2018 electoral violence indicated that the violent demonstrations were incited and perpetrated through the irresponsible use of social media (Commission of Inquiry, 2018). In the run up to the 1st of August 2018 violence, citizens took to social media to announce election results before their official announcement by the Zimbabwe Electoral Commission (ZEC). Moreover, messages of alleged rigging also circulated over social media platforms. This irresponsible use of social media created tension and political intrigue, which culminated in the violent protests that characterised the city of Harare on the 1st of August 2018. An election is one of the fundamental manifestations of democracy and having this important exercise compromised through irresponsible use of social media is not only a threat to democracy but also promotes political instability. On the other hand, we should not lose sight of the fact that citizens had lost faith in ZEC’s ability to deliver a credible election, and in a polarised media environment, citizens found social media platforms as the only avenue to have their voices heard.

In January 2019, Zimbabwe witnessed a wave of violent protests in all major cities after the President had announced an increase in fuel prices (News24, 2019). Social media platforms were used to plan and to disseminate information on the planned protest a day before the violent protests. The citizens’ agitation was compounded by other socio-economic challenges such as shortage of fuel, food and medicine (News24, 2019); hence, the citizens’ discontent seemed to have been mounting for some time. During the violent protests, citizens posted real-time videos of the violent protests on various social media platforms, thereby fuelling further protests. Prominent activists such as Evan Mawarire were at the forefront, posting videos of the ongoing protest on social media platforms and he was arrested again for incitement to commit violence (News24, 2019). The violent protests had the following consequences: loss of lives (12 civilians and one police officer); destruction of property; and massive looting in shops. With the rapidly deteriorating security situation, the government took a drastic measure of shutting down internet (Zimbabwe Independent, 2019), which will however be analysed later in this paper.

Social media platforms have also been instrumental in the spread of fake news to citizens, with some of the news intended to cause panic and despondency. On several occasions, the government and its agencies had to dispel fake news that would have emanated from social media. For example, on the 13th of October 2019, citizens received fake news relating to an increase in fuel prices and the news purported to have come from the Zimbabwe Energy Regulatory Authority of Zimbabwe (ZERA), which regulates fuel prices in Zimbabwe. Given that a previous announcement of a fuel price hike had sparked widespread violence in January 2019 (News24, 2019), the fake message could have been intended to have the same effect. The message, however, created panic, with motorists scrambling to buy the fuel before the purported new price would come into effect,
whilst fuel operators withheld their fuel in anticipation for a price hike. ZERA had to dispel the fake social media news through the State broadcasting media, though this came a bit late. In September 2019, there was a fake social media message claiming that the Reserve Bank of Zimbabwe (RBZ) was printing new currency and the unknown author of the message even went to the extent of showing the specimen of the fake currency. This caused fear on the citizens, with some citizens heavily criticising the government, given the negative implications of introducing a new currency without first addressing the macro-economic fundamentals. Again, the RBZ had to dispel the misinformation through the state-run media. In October 2017, a ministerial taskforce that had been tasked to investigate price hikes and panic buying in the country revealed that social media platforms were the cause (Daily News, 2017), and on several occasions social media were awash with fake news on purported imminent commodity shortages, thus leading to panic buying and price hikes. From the above examples, it can be seen how the spread of fake news can have serious implications on the economy.

The political and diplomatic fronts have also been at the receiving end of the irresponsible use of social media. For example, on the 1st of April 2020, social media platforms were awash with fake news indicating that the Zimbabwean President, Emerson Mnangagwa, had tested positive for COVID-19 virus and was under quarantine. Given the fear that had gripped the whole world over the virus, this message was intended to further induce fear and panic among Zimbabweans, as it would portray the government’s failure to deal with the pandemic. During the run up to the 2018 general elections, social media platforms got dominated by people who claimed to have well-connected sources with inside information about what was going to happen (Media Monitor, 2018) and this brought about political intrigue in the nation. The Zimbabwe Electoral Commission and its top officials were subject of numerous fake news on unproven allegations of vote rigging (Media Monitor, 2018) and this perhaps worsened the political climate that characterised the 1st of August 2018 protests. In another social media message that had diplomatic ramifications, a fake message purportedly emanating from South African President Ramaphosa indicated that the President had ordered all foreign nationals residing in South Africa to leave the country before 21 June 2020 due to increasing cases of COVID-19. Part of the message, which started circulating on the 7th of April 2020 as breaking news read;

“... and the president is asking all foreigners to vacate so that the country can (be) left with its only citizens who will be given free food, water, electricity and free rent. The president says its government cannot manage to provide these free things to foreigners since the number of foreigners is high compared to other countries. The president is also asking presidents from foreign countries to start sending buses and aeroplanes to carry their citizens especially from Zimbabwe, Mozambique, Zambia, Democratic Republic of Congo ... .”

The message trended in most WhatsApp group and individual conversations, with most people enquiring on the authenticity of the message. Most Zimbabweans, whose relatives were either working or residing in South Africa, were sent into panic, especially in the absence of communication to dispel the fake news. Given the previous negative effects of such inflammatory statements in South Africa (Citizen Research Centre (CRC), 2019), most of the citizens who had sight of the fake message reminisced the xenophobic attacks that characterised South Africa in 2015 and 2019.

Whilst this paper relates to national security mainly in the context of high politics, social media also have implications on human security. Social media platforms have been used to commit other various criminal activities in Zimbabwe. Human trafficking is one of the areas in which social media have played a significant role. During the year 2016, Zimbabwe witnessed a rise in human trafficking cases, with the most prominent cases involving trafficking of would-be housemaids to Kuwait (Machakaire, 2017). The victims were mainly recruited through Facebook and WhatsApp platforms, and they were later turned into slaves and prostitutes upon arrival in Kuwait. Using the same modus operandi, Machivenyika (2017) also reports that over 200 human trafficking victims had been trafficked to Kuwait and Saudi Arabia, where they were
forced to engage in prostitution and labour enslavement. Social media platforms have also been used to commit other harmful activities such as harassment and distribution of pornographic material (The Patriot, 2017). In February 2020, police in Bulawayo (Zimbabwe’s second largest city) arrested four men for peddling pornographic material through social media. The accused persons were either possessing, or distributing pornographic material using Facebook, Twitter or Instagram accounts (Tshili, 2020). In what seems to be an inability by the country’s police to deal with such a case, the companies that run the social media platforms raised the red flags and alerted the Zimbabwean law enforcement authorities. Revai (2019) also noted a significant rise in revenge pornography, with the social media platforms being used in the perpetration of this vice. Revenge pornography has serious implications on the citizens’ right to privacy.

4. The legal framework for social media operations in Zimbabwe

Whilst there are several measures to deal with social media threats to national security, enactment of relevant laws seems to be one of the most adopted strategies across the globe. This section accesses Zimbabwe’s regulatory framework in light of the threats posed by social media on national security. The section starts by highlighting the constitutional provisions that have a bearing on social media operations. It is also important at this point to highlight that there is no law that specifically deals with social media threats to national security. However, the paper reviews some statutes and provisions that have been invoked in light of social media threats. The analysis is two-pronged; it looks at provisions that promote social media usage and then the provisions that seem to curtail the social media threats.

4.1. Social media and the constitution

The Constitution of Zimbabwe guarantees freedoms and this guarantee applies both in the physical space and virtual space. Section 57 of the Constitution provides for the right to privacy and Section 57 (d) specifically provides that people have a right not to have the privacy of their communications infringed. This is an unambiguous prohibition of spying and interference on the citizens’ communications, be it in the physical world or virtual world. Section 58 of the Constitution provides for the freedom of assembly and association, while section 59 provides for the freedom to demonstrate and petition. As earlier explained, social media platforms facilitate the enjoyment of these rights, as citizens can gather on these platforms to organise and coordinate protests. It is important to highlight that Section 59 expressly states that the freedom to demonstrate and petition must be exercised peacefully. Thus, despite the guarantee for protest, any form of violence during the protests will render the protests unconstitutional. However, in practice, the police have on numerous occasions denied the citizens their freedom to gather and demonstrate, citing national security concerns. In a move that attracted worldwide condemnation in July 2020, several journalists and civic society activists were arrested by police for organising protests against corruption on social media platforms.

Another section which has a direct bearing on social media operations in Section 61, which provides for the freedom of expression and freedom of the media. Section 61 (a) provides for freedom to seek, receive and communicate ideas and other information, while Section 61(b) provides for freedom of artistic expression and academic freedom. Again, social media platforms facilitate the enjoyment of these important rights. The above constitutional provisions seem to support the social responsibility theory, which stipulates that media operations should be independent from the government (Philip, 2001), with the government only setting parameters for the media operations. However, the Constitution prescribes the following under Section 61 (5): incitement to violence; advocacy of hatred or hate speech; malicious injury to a person’s reputation or dignity; or malicious or unwarranted breach of a person’s right to privacy. Given the longstanding finding that social media has been used to incite violence (Cuman, 2012; Liaropoulos, 2013; Tufekci, 2017) the Constitution of Zimbabwe seems to take cognisance of this reality. While it can be inferred that Section 61 (5) is interfering with the social media, what the section is actually advocating for is the responsible use of social media. However, notwithstanding the presence of these clearly articulated rights, several political activists and journalists in Zimbabwe have been arrested for expressing their anger over corruption and bad governance.
Another important right is the right of access to information (Section 62). The section provides that every citizen has the right of access to any information held by the State or by any institution or agency of government at any level, in so far as the information is required in the interests of public accountability. Thus, social media provide a channel through which this right is exercised. Government departments such as the police, as well as key government employees such as ministers have social media accounts where they update citizens on the developments in their respective departments and on issues that affect the citizens’ socio-economic wellbeing. However, it should be noted that where citizens feel that they are not getting adequate information from the government, they resort to social media news, with the state having to contend with negative consequences of social media news. In an effort to curtail some of the criminal activities related to access of information, Section 62 (4) provides that legislation must be enacted to give effect to this right, but may restrict access to information in the interest of defence and public security, though the restriction has to be fair, necessary and justifiable in a democratic society.

4.2. Other applicable laws for social media threats to national security

With the absence of laws which specifically deal with social media threats, several Acts of Parliament have been invoked to deal with some of the threats posed by social media on national security. Perhaps the first attempt to deal with threats posed by various communication platforms in Zimbabwe was the enactment of the Postal and Telecommunications Act [Chapter 12:05] of 2000, which, under section 88, prohibits the sending of messages that are: grossly offensive; indecent; obscene or threatening; false; or causing annoyance, inconvenience or needless anxiety. The same section imposes a fine not exceeding level five or imprisonment for a period not exceeding 6 months or both. Though this section has mainly been invoked on threats that relate to telephone and postal communication, it seems to be relevant in the fight against social media threats as well. In what seems to be a provision that allows for monitoring of communication, section 98 provides for interception of communication which will afford evidence of commission of crime.

The Official Secrets Act [Chapter 11:09] was passed in 2001, and it stipulates that documents that relate to the state security, national defence, or internal public order shall not be released into the public sphere. Given that such documents can be released into the public domain through social media platforms, the Act also becomes relevant, though the law enforcement agents seem reluctant to invoke the relevant provisions on social media related threats. The rationale for having such an Act was vividly evident in the case of the publication of USA government cables from diplomatic missions all over the world by a whistleblower site known as Wiki leaks, which resulted in mistrust, suspicion and hostility towards the US government (Mhiripiri & Chikakano, 2017). Thus, even developed nations contend that official state secrets cannot be released into the public domain.

In 2002, there was a landmark development in the legislative framework for media-related activities. The Access to Information and Protection of Privacy Act [Chapter 10:27] (AIPPA) was promulgated and among other objectives, provides for: the right of access to information held by public bodies; protection of access to certain information; and the regulation of mass media. Sect 17 of the AIPPA provides for protection of information whose disclosure will be harmful to law enforcement process and national security. According to the Zimbabwe Democracy Institute (2017), AIPPA provisions were put in place to control mainly the outflow of information in privately owned media houses so as to create doomed mindsets of citizens. Since its inception, calls have been made for the legislative authority to repeal AIPPA, as some of its provisions are deemed to be in violation of the Constitution. Following incessant pressure from the courts, civic society and the citizens at large, the Cabinet resolved to repeal the AIPPA in 2019, though the legislature is yet to formalise the cabinet decision.

Perhaps the law that has been mostly invoked by law enforcement agents on social media related threats is the Criminal Law [Codification and Reform] Act [Chapter 9:23] of 2004 (hereinafter called the Criminal Law Code). Chapter 3 of the Criminal Law Code provides for the crimes
against the State, whilst Chapter 4 provides for crimes against public order. Among the commonly, yet controversial, provisions that have been invoked include: Section 22- Subverting constitutional government; Section 23- Insurgency, banditry, sabotage and terrorism; Section 30- Causing disaffection among Police force or Defence Force; Section 31- Publishing or communicating information prejudicial to the State; Section 33- Undermining or insulting the authority of the President; and Section 36- Public violence. It is important to note that irresponsible use of social media can have a bearing on all the above statutory provisions. It is interesting to note that Section 31, which criminalises publishing of information prejudicial to the State and Section 33, which criminalises undermining the authority of the President, have long been ruled as unconstitutional by the Constitutional Court of Zimbabwe (Murwira, 2013). However, the legislative authority is yet to affect the Constitutional judgement through corrective action.

In the famous case of Baba Jukwa, whose Facebook posts created political intrigue and panic in the country, a suspect was arrested in June 2014. The law enforcement agents preferred two charges, namely; subverting constitutional government (Section 22), or alternatively attempting to commit an act of insurgency, banditry, sabotage or terrorism (Section 23) (Charles, 2014). It should be noted that social media do not directly lead to commission of some of the crimes spelt out in the Criminal Law Code, but may be used as platforms for inciting citizens to engage in the prohibited acts. In the case involving cleric Evan Mawarire of the #thisflag and #ShutDownZimbabwe movements in 2016, the law enforcement agents preferred a charge of incitement to subvert a constitutional government (Section 22), which attracts up to 20 years imprisonment. During the January 2019 violent protests, Evan Mawarire was charged with incitement to commit public violence, which he allegedly committed through social media platforms. Whilst it was easy to deal with those who actually participated in the violent protests, it was difficult to deal with those who incited the violence through social media platforms. Up to now, the cases involving Baba Jukwa and Evan Mawarire have not been finalised by the courts, highlighting what could be a challenge in the current legal framework to deal with social media threats to national security.

In another significant development, the Interception of Communications Act [Chapter 11:20] was passed in 2007. The Act provides for the lawful interception and monitoring of certain communications in the course of their transmission. The Act also provides for the establishment of a Monitoring and Interception of Communication Centre, which has the power to oversee the traffic in all telecommunication services and to intercept phone calls, emails and faxes, all under the pretext of national security. While interception of communication seems to be contrary to Section 57 (d) of the Constitution (right not to have private communications infringed), Section 86 (2) (b) of the Constitution provides for the limitation of the rights in the interests of defence, public safety and public order. In a widely condemned move, the Interception of Communications Act was invoked by the government to shut down internet during the January 2019 violent protests, wherein there was a social media blackout for 6 days after the government ordered all network service providers to shut down internet (Matshazi, 2019). While the internet shut down was done to stop protestors from organising, this was a violation of citizens’ right of access to information and freedom of speech. Internet was only restored after the Media Institute of Southern Africa (MISA) approached the court, with the High Court ordering immediate restoration of internet services. While some argue that the shutdown was necessary to control a degenerating security situation, the internet blockade was widely condemned and the move to shut down internet put a dent on the country’s human rights record. Moreover, there have been numerous arguments against the idea of intercepting citizens communication (for example, Zimbabwe Democracy Institute, 2017; Matshazi, 2019; Zimbabwe Independent, 2019), chiefly due to the human rights implications of such a move.

An analysis of the above statutes and the relevant statutory provisions reveals the daunting task of dealing with the social media threats to national security. Where charges have been preferred against the accused persons, the cases are taking long to complete due to the complexities
involved. Similarly, blocking social media sites, monitoring of social media and interception of communication have also been condemned on human rights grounds. The possible explanation for the current conundrum could be the absence of a single piece of legislation that regulates social media activities in light of social media-induced threats to national security. Perhaps the solution lies in the enactment of the Cyber Crime, Security and Data Protection Bill. The Bill, which was in the pipeline since 2014, seems to address most of the threats that are posed by social media. Among other issues, the Bill: provides penalties for the transmission of data messages inciting violence and damage to property; provides for measures to address the production and dissemination of racist and xenophobic material; provides for the protection of citizens against cyberbullying and harassment; and provides for measures to curb transmission of pornographic material. Another controversial provision relates to the lawful seizure of devices such as cell phones for the purpose of investigation, as well as the interception of any electronic communication. Given that the Bill is yet to go through the necessary legislative processes, it would be prudent to critically evaluate it once it sees its day as an Act of Parliament.

5. Conclusions

It is without doubt that the upswing in the adoption of social media as communication platforms has brought a dilemma on the government and its agencies. The resultant threats have been huge, chief among them being facilitation of violent protests. Facebook has mainly been used to issue subversive statements and to urge the citizens to revolt against the government. The inherent challenge in controlling social media communication has facilitated the spread of fake news on social media platforms. Such fake news has negative economic, political and social ramifications and is intended to cause panic and despondency in the nation. Moreover, social media platforms have also facilitated human trafficking, which on its own is a global threat to humanity. The government finds itself in a difficult conundrum, where they have to balance between harnessing the positive aspects of social media and dealing with the threats that the social media bring. Regulatory control seems to be the most viable option to deal with social media threats. Whilst the Constitution sets a positive framework, especially from a human rights perspective, other statutory instruments seem to be inadequate or ineffective in dealing with social media threats. In most of the cases where suspects were arrested for social media-related offences, no conviction has been secured, thus confirming the possibility of loopholes in the current legal framework. Perhaps the most viable option is to promulgate the Cyber Crime, Security and Data Protection Bill, which if passed into law, will address some of the challenges with the current legal framework. While there is much talk on the impending law, the legislative authority still faces the dilemma of enacting a law which addresses the social media threats, but within the confines of the Constitution. Arguably, balancing the two (enacting the law and adhering to the constitutional provisions) will be a mammoth task.

Author details
Ishmoel Mugari1
E-mail: ishiemugari@gmail.com
1 Bindura University of Science Education, Bindura, Zimbabwe.

Citation information
Cite this article as: The dark side of social media in Zimbabwe: Unpacking the legal framework conundrum, Ishmoel Mugari, Cogent Social Sciences (2020), 6: 1825058.

References
(2004a) Criminal Law [Codification and Reform] Act (Chapter 9:23), Government Printers.
Access to Information and Protection of Privacy Act (Chapter 10:27) No 5/2002, Government Printers.
AliZabi, K. A. T., & Tomic, D. (2010). New Security paradigm: The use of social networks as a form of threat to the national security. Ann. Disaster Risk Sciences, 1(1), 27–33.
Bakir, V., & McStay, A. (2018). Fake News and the Economy of Emotions: Problems, Causes, Solutions. Digital Journalism, 6(2), 154–175. doi:10.1080/21670811.2017.1345645
Borau, S., & Wamba, S. F. (2019, April). Social Media, Evolutionary Psychology and ISIS: A Literature Review and Future Research Directions. In World conferences on Information Systems and Technologies (pp. 143–154).
Bradshaw, S., & Howard, P. N. (2018). Truth and Trust: A Global Inventory of Organized Social Media Manipulation. Computational Propaganda Research Project. Oxford Internet Institute.
Bruce, R. L. (2011). Social Media and Disasters: Current Uses, Future Options, and Policy Considerations. CRS Report for Congress.
Charles, L. (2014). Sunday Mail Editor is Baba Jukwa. The Standard, 22(June), 2014.
Citizen Research Centre (CRC). (2019). Xenophobia on social media in South Africa: 2011– present day. Vibrand, 13(October), 2019. Retrieved from vibrand.co.za/xenophobia-on-social-media/
Constitution of Zimbabwe, Amendment (No 20) Act of 2013. Government Printers.

Cuman, K. (2012). The Role of Internet and Social Media in International Relations: Arab Revolution of 2011. Daily News. (2017). Ministers blame social media for panic buying. Daily news, 14(October), 2017. Retrieved from dailynews.co.zw/articles-2010-10-14-ministers-blames-social-media-for-panic-buying/

Fitsanakis, J., & Bolden, M. (2012). Social Networking as a Paradigm Shift in Tactical Intelligence Collection. Mediterranean Council for Intelligence Studies Yearbook, 1(1), 28–40. Retrieved from rieas.gr/images/mcis2012.pdf

Forster, P. (2013). Bogus AP tweet about explosion at White House wipes billions off US markets. The Telegraph, 23(April), 2013. Retrieved from https://www.telegraph.co.uk/finance/market/10013768/Bogus-AP-tweet-about-explosion-in-the-White-House-wipes-billions-off-US-markets.html

Fuchs, C. (2013). Social media: A critical introduction. SAGE.

Ghonim, W. (2012). Revolution 2.0. The Power of the People Is Greater Than the People in Power. Houghton Mifflin Harcourt.

Hodge, N. (2010). U.S. Diverts Spy Drone from Afghanistan to Haiti. Wired Magazine, January 15, 2010.

Interception of Communications Act, Chapter 11: 20. Government Printers.

Kimutai, J. K. (2014). Social Media and National Security Threats: A Case Study of Kenya, Master of Arts in International Studies Thesis, University of Nairobi.

Klang, M. (2011). “Disciplining social media: An analysis of social media policies in 26 Swedish municipalities”. First Monday, 16(8).

Liarpoulos, A. (2013). The challenges of social media intelligence for the intelligence community. Journal of Mediterranean and Balkan Intelligence, 1(1).

Lumpa, T. G. (2014). The Effects of Social Media on National Security within the United States. Published Master of Science in Cyber security Thesis, Utica College.

Machakaire, T. (2017). Zimbabwe now major cocaine market. Daily news, 14(May), 2017.

Machivenyiwa, F. (2017). Over 200 human trafficking victims back in Zimbabwe from Kuwait and Saudi Arabia. The Herald, 7(April), 2017.

Matshazi, N. (2019). Digital rights: Lessons from Zimbabwe’s Internet shutdown. Newsday, March 2019.

Media Institute of Southern Africa (MISA). (2018). Digital Rights Report. MISA.

Media Monitor. (2018). Change of Guard, Zimbabwe Media: Mugabe to Mnangagwa Transition.

Mhiriipi, N. A., & Chikakana, J. (2017). Criminal Deformation, the Criminalisation of Expression, Media, and Information Dissemination in the Digital Age: A Legal and Ethical Perspective. In N. A. Mhiriipi & T. Chari (Eds.), Media Law, Ethics and Policy in the Digital Age (pp. 1–24). IGI Global.

Mujere, J., & Mwotwaru, W. (2015). Citizen Journalism and National Politics in Zimbabwe: The case of 2008 and 2013 Elections. In B. Mutsivai (Ed), Participatory Politics and Citizen Journalism in a Networked Africa: A Connected Continent (pp. 1–15). Palgrave, Macmillan.

Muwira, Z. (2013). Concourt strikes down sections of Statute Law. The Herald, 31 October.

Nyangi, J. (2017). Social Media customer service. Newsday, August 2019.

Official Secrets Act (Chapter 11:09) 22/2001. Government Printers.

Poniatoski, S. The social media challenge to national security: Impact and Opportunities. A conceptual review. IDSA Monograph Series No 55, November 2016.

Philip, M. N. (2001). Social Responsibility and Commercial Broadcast Television: An Assessment of Public Affairs Programming in JMM, The International Journal on Media Management, 3(4), 20–34.

Report on the Commission of Inquiry into the 1st Of August 2018 Post Election Violence. http://www.postelectionviolencecommission.gov.zw/2019/01/18/legality-of-zms-internet-shutdown/
