Surveillance and Monitoring in the Social Media Era: Threats and Opportunities to Democratic Processes in Southern Africa

Tawanda Mukurunge, Neo Tlali, Takura Bhila

Limkokwing University of Creative Technology, Lesotho Campus, Maseru, Lesotho

ABSTRACT

Social media platforms are viewed as all progressive in opening up democratic spaces the world over. In the Middle East and North Africa region, social media platforms are regarded as key to the Jasmine Revolution that resulted in the fall of some regimes widely regarded as repressive by the international community. In Southern Africa, the hashtag movements saw youth shrugging off political apathy to challenge the establishment. Information Communication Technologies are refreshingly enticing the youth to participate and revitalize politics in the sub region. However, regimes in the sub region, traditionally comfortable with the hegemonic stringent hold on mainstream media, are becoming uncomfortable with these new developments and have resorted to legislation that threaten freedom of expression by citizens on social media as well as surveillance of citizens. This study is therefore going to establish societal views on state surveillance and monitoring of citizens' activities on social media. This is going to be executed through in-depth interviews with media practitioners, scholars, political analysts, policy makers and ordinary users of social media platforms. Findings will be presented and analysed qualitatively and thematically.

KEYWORDS: social media, surveillance, monitoring, hegemony, mainstream media

INRODUCTION

Social media platforms are an exciting prospect for prodemocracy forces such as civil society organizations and the tech savvy generation. However, this exciting prospect is regarded as a threat by some political establishments, both repressive and democratic in outlook. US scholars Zuckerman and Sauter (2014) studied and published on the discomfort expressed by the US government with online activities to the extent that online activists are labeled terrorists or hackers and if convicted of such a crime categorized as cyber terrorism or hacking, the fine and prison sentence is prohibitive. Arora (2010) writes about how surveillance by state authorities has been made easy by the ready availability of information on individuals the world over due to the big data phenomenon. Scholars who have studied the big data question have established how internet users innocently feed the internet with their personal details and how this technology can create profiles of individuals without the individuals' knowledge of such. Shirky (2008) exemplified this vulnerability of innocent internet users by narrating how an individual who lost a mobile phone managed to recover the property when a friend assisted her to track down the person who ended up possessing the phone through the internet profiling of individuals as well as through mobilization and campaigning via internet platforms. This internet compilation of individuals' profiles is the one exploited by state agents to monitor and survey activities of individuals of interest to their purposes. This study is going to explore how the internet surveillance and monitoring of marked individuals is a threat to both freedom of expression and personal freedom of citizens in their exercising of the right to personal freedom. At the same time, the internet, through social media platforms, provides opportunities for individuals to circumvent gate keepers in communication and express themselves and mobilize to achieve desired ends.

Statement of problem

Social media platforms have presented opportunities for previously marginalized communities to participate without limits such as the ones paused by gate keeping in mainstream media. However, there are challenges in that authoritarian states are using the same social media platforms to survey on their citizens by monitoring their political communication activities. This presents physical danger to known and marked political activists in these environments mainly due to the existence and easy accessibility of big data on individuals.

Study objectives

The study sought to establish the opportunities for citizens in political communication previously inaccessible due to control by authorities such as through editorial policies and gate keeping. The study also sought to establish hidden dangers not apparent to innocent hapless social media users

that endanger them through monitoring of their online activities by their governments.

Theoretical framework
The theory framing this study is the digital public sphere theory. Sampedro and Martínez Avidad (2018) say that the digital public sphere theory emanated from the historical view of social mobilizations coordinated by digital technologies. The public sphere is that space where citizens meet to discuss issues of socio-economic and political concern apart from the for a created by the state such as parliament. This is a coming together of citizens of their own volition and on the digital public sphere; this coming together is deliberated via the internet and the different platforms available on it.

Literature review
On social media and governance, Khan, Swar, and Lee, (2014) write that social media are becoming an important intermediary for interaction between governments, governments and citizens, and governmental agencies and businesses. They say that this is due to the unique characteristics of social media: openness, participation, and sharing. They go on to say that, however, despite rapid adoption, a growing concern and skepticism regarding the use of social media exists in the public sector. Social media platforms are particularly popular with young users, study testifies.

On social media and youth users, Shava and Chinyamurindi (2018) write that Youths have been found to utilise and adopt information communication technology (ICT) faster than any other population cohort. This has been aided by the advent of social media, especially Facebook and Instagram as platforms of choice. Calls have been made for more research (especially in rural communities) on the usage of ICT platforms such as social media among the youth as a basis for interventions that not only allow for better communication but also for learning.

Writing about how businesses in South Africa harness and utilize social media platforms in South Africa, van der Ross (2015) says that in recent years, the information systems / information technology industry has been one of the most fast growing industries. He also says that regularly, existing technologies are being upgraded and new technologies are being introduced within the industry. van der Ross continues to say that for these reasons, business institutions have to stay abreast with market trends and understand what the market is doing. Since the inceptions of social media, a relatively new phenomenon within industry, institutions have to get on board in terms of using these technologies simply because of what the customers are doing.

Social media is also impacting the tourism industry positively. van der Bank (2015) writes that the role and use of social media in travelers " decision making and tourism operations and management are widely discussed. She continues to say that the strategic importance of social media are high for tourism competitiveness as the online world is rapidly evolving and some companies may embrace new technologies due to the pressure to be digital but are not thinking about what it means to the business in a virtual environment. van der Bank also says that the phenomenon of social networking and the development of social media (web-based and mobile technologies that turn text

communications into active dialog) has been the most dramatic development in the information age over recent years.

Writing about surveillance and monitoring of citizen social media activities in the USA, Electronic Privacy Information Centre (EPIC) (2018) says that social media monitoring software (SMMS) has significantly expanded over the past several years. Fortune 500 companies, politicians, law enforcement, federal agencies, defense contractors and even the military are purchasing SMMS products, such as XI Social Discovery, Geofeedia, Dataminr, Duanmi, MediaSonar, and SocioSpyder to name a few.12 The CIA even has a venture fund, In-Q-Tel, that invests in SMMS technology (epic.org, 2018). The EPIC document goes on to say that through a Freedom of Information Act request in 2011, EPIC was the first to uncover information about social media monitoring by a federal agency. In EPIC v. DHS, EPIC obtained nearly 300 pages of documents about the Department of Homeland Security's monitoring of social media data. 2 The documents clearly showed that the monitoring program was more expansive than DHS had communicated to the public. DHS secretly tracked public comments on policy debates related to the department activities.

Kibby and Fulton (2016) write that the millennial generation seems to be habituated to having immediate access to information, including essentially private information on people of interest to them. They continue to say that social media has accustomed them to watching and being watched. They cite Albrechtslund (2013) who describes this type of surveillance as "participatory surveillance", where people willingly keep watch on each other through social media. They illustrate with an example of an anonymous focus group and online survey of 80 Australians aged between 18 and 34 investigated their use of participatory surveillance, that is, of their surveillance techniques on others and their awareness of the level of surveillance they themselves are under. The results reveal that while these young people were concerned about the privacy and security of their own personal information, they had come to rely on being able to access the personal information of others.

Mateescu, Brunton, Rosenblat, Patton, Gold, and Boyd (2015) say that law enforcement monitoring of social media is a widespread and growing practice. In 2014, a vendor's online survey of more than 1,200 federal, state, and local law enforcement professionals found that approximately 80 percent used social media platforms as intelligence gathering tools.2 The adoption of these new tools may not come as a surprise given their low cost compared to other forms of surveillance. But their adoption also reflects a broader trend: law enforcement's response to public pressure to investigate crimes online. For example, after a number of highly publicized violent attacks — from the Boston Marathon bombing, to the killing of churchgoers in Charleston, to mass shootings on school campuses – journalists have unearthed social media profiles full of warning signs: posts about hate, weapons, and more. Those discoveries have contributed to mounting pressure on law enforcement to do more to identify potential offenders before they act.

Methodology
The study used qualitative methods to gather the information, present the findings and analysis of the findings. Cresswell (2009) says that qualitative research is a

means for exploring and understanding the meaning individuals or groups ascribe to a social or human problem. The study used interviews face to face and telephonically in order to glean citizens' understanding of the problem of state surveillance and monitoring of citizens' online activities. Face to face interviews have got the advantage of allowing the interviewer to read into some nuances such as non verbal communication cues that cannot be detected with other means of data gathering.

Findings
Responses from journalists
Journalists expressed the view that state surveillance of citizens is real as they testify to the hacking of their social media accounts and emails by suspected state intelligence operatives. They say that they can only tell when there is evidence of hacking of their accounts but suspect that the monitoring can even be deeper considering that the state has got the resources to access sophisticated gadgets that can be operational without ordinary citizens being conscious.

Responses from media scholars
Media scholars said that the west has been monitoring the activities of suspicious citizens since the cold war era and it got intense after the September 11 2001 terrorist attacks on the US. The academics also said that governments can have easy access to surveillance technology and that some of this information is available free of charge online due to the big data phenomenon. They went on to say that a lot of people tend to post finer personal details which end up accessible to anyone with access to Google. They say that to anyone interested in monitoring anyone, the information is readily online so long that person has uploaded it and the person's interests, associates and exchanges can reveal a lot about the individual. Other scholars, however, said that machines alone cannot effectively monitor citizen activities without spies on the ground.

Responses from political analysts
Political analysts said that local state security agencies are not that equipped either with the skills or equipment to monitor the online activities of every citizen. They said that, as a matter of fact, the local cyber security is very weak. They said that reported cases of cyber crime can go for ever without being resolved due to lack of capacity by the state to solve them therefore surveillance by the state on online activism is almost nonexistent.

Responses from students of journalism
Students of journalism expressed the view that it is not easy or the state to monitor the online activities of citizens because it is not well equipped with the technology to do so. They went on to say it is easy for the state to identify and persecute online anti state activists on Facebook and YouTube, but not on the other social media platforms. They also said that even on Facebook, the state can only vent frustrations by threatening suspected activists but they do not have the capacity to block or delete posts. They gave the example of the Makhaola Qalo Facebook page which continues whistle blowing against those in power and for years now the authorities have not been able to disable the page or arrest the person/people posting on the page. The students continued to say that with WhatsAapp and Instagram, there is no way the state can break into those communications because they are said to be end-to-end. This

means the ownership of WhatsAapp and Instagram are centralized and states cannot have access to the content of WhatsAapp and Intagram accounts.

Responses from citizen of social media platforms
Citizens responded that they do not think the state has got the capacity to monitor activities of ordinary citizens online because it is beyond the state's capacity. They said that they believe that the citizenry is free to express their views, political and otherwise, and that the state actually benefits from this feedback from the constituencies. They however believe the state does not have enough time to do any surveillance and monitoring of citizen online activities.

Discussion of findings
It is apparent that when it comes to internet and social media participation, journalists feel that state monitoring and surveillance is real and threatens freedom of expression. Hintz (2012) writes that developments in communication through the WikiLeaks releases and the Arab Spring have demonstrated the capacities of individuals and movements in advancing free expression, transparency and social change through the use of online and social media. However they have also highlighted new sets of challenges and threats that interfere with, and restrict, such media uses. Journalists are therefore conscious of the potential presented by social media platforms to enhance freedom of expression but are also aware of the threat through state surveillance and monitoring of the social media space by the state.

Media scholars' fears of the big data phenomenon are echoed by Schirch (2019) who says that alarming stories about social media hit the news almost every day with headlines announcing violations of user privacy as social media companies collect and sell our personal information; Russian troll farms attempting to suppress the African American vote in the US election to assist the Trump campaign; and Facebook executives delaying, denying, and deflecting responsibility for the vast impacts of their platform on democracy, rights to privacy, polarisation and personal safety. Ordinary citizens keep on posting their personal information that might end up being used to their disadvantage for surveillance purposes and invasion of their privacy. The citizens interviewed however are oblivious to this fact and have faith in the liberatory and democratization opportunities of social media platforms.

Levinson-Waldman (2018) writes that Technology is transforming the practice of policing and intelligence. In addition to the proliferation of overt surveillance technologies, such as body cameras and license plate readers, there is a revolution playing out online where domestic law enforcement agencies are using social media to monitor individual targets and build profiles of networks of connected individuals. Political analysts and students of journalism underestimate the potential of state agencies on surveillance of civilian online activities and it is very dangerous even for civilian personal safety.

Isaac (2019) writes that Mark Zuckerberg, Facebook's chief executive, plans to integrate the social network's messaging services — WhatsApp, Instagram and Facebook Messenger — asserting his control over the company's sprawling divisions at a time when its business has been battered by scandal. Mr. Zuckerberg has also ordered that the apps all

incorporate end-to-end encryption, the people said, and a major step that protects messages from being viewed by anyone except the participants in a conversation. This communication is in line with student observations that social media platforms have the capacity for opening up the democratic state, that is, if citizens can freely participate without state agencies snooping in on their activities.

However, study reveals that states are increasingly investing in citizen online surveillance and monitoring. Bradshaw and Howard, (2017) write that cyber troops are government, military or political party teams committed to manipulating public opinion over social media. Cyber troops are a pervasive and global phenomenon. Many different countries employ significant numbers of people and resources to manage and manipulate public opinion online, sometimes targeting domestic audiences and sometimes targeting foreign publics.

Recommendations

The study recommends that citizens should be sensitized to the dangers of divulging sensitive personal information as interested groups from government to business prey on big data saved on individuals' profiles. This makes it easy for rogue state agencies to survey on the activities of unsuspecting citizens. The study also recommends that citizens identify those social media platforms whose security can easily be breached and be careful about what they post. Citizens should exercise caution when interacting with and on social media platforms.

Conclusion

The study sought to establish citizens' perceptions of social media use; opportunities and threats through state surveillance and monitoring. It was discovered that the younger generation view social media platforms as liberator and do not believe that the state has got the capacity to survey and monitor on citizen activities online. The scholars and journalists are skeptical when it comes to online participation because of the perceived dangers paused by exposing oneself through divulging too much personal information which is captured by commercial organization and amalgamated into big data which is exploited by rogue states for monitoring and surveillance purposes.

References

[1] Bradshaw, S. and Howard, P. N. (2017). Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation. *Computational Propaganda Research*. Working paper no. 2017.12

[2] Cresswell, J. W. (2009). Research design: qualitative, quantitative and mixed methods approaches SAGE.

[3] Electronic privacy information centre. (2018). Social Media Monitoring: Government Surveillance of Public Space. Spotlight on Surveillance epic.org.

[4] Hintz, A. (2012). Challenges to Freedom of Expression in the Digital World: Lessons from WikiLeaks and the Arab Spring. *ESSACHESS. Journal for Communication Studies*, vol. 5, no. 1(9).

[5] Isaac, M. (2019). Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger. The New York Times.

[6] Khan,G. F., Swar, B. , and Lee, S. K. (2014). Social Media Risks and Benefits: A Public Sector Perspective. *Social Science Computer Review* 2014, Vol. 32(5).

[7] Kibby, M. and Fulton, J. (2015). Surveillance, Privacy, and Social Media. *Conference: Association of Internet Researchers Conference* At: Phoenix, Az.

[8] Levinson-Waldman, R. (2018). Government Access to and Manipulation of Social Media: Legal and Policy Challenges. *Howard Law Journal*. Vol. 61 No. 3

[9] Mateescu, A., Brunton, D., Rosenblat, A., Patton, D., Gold, Z, and Boyd, D. (2015). Social Media Surveillance and Law Enforcement. Data & Civil Rights: A New Era of Policing and Justice.

[10] Arora, P. (2010). Dot com mantra: social computing in the Central Himalayas. Ashgate.

[11] Sampedro, V. and Martínez Avidad, M. (2018). The Digital Public Sphere: An Alternative and Counter hegemonic Space? The Case of Spain. *International Journal of Communication* 12(2018)

[12] Shava, H and Chinyamurindi W. T. (2018). Determinants of social media usage among a sample of rural South African youth. *South African Journal of Information Management* 20(1).

[13] Schirch, L. (2019). Mapping Responses to Social Media Threats. *Toda Peace Institute*. Policy Brief No. 38.

[14] Shirky, C. (2008). Here comes everybody. Penguin Books.

[15] van der Bank, C.M. (2015). The impact of social media: advantages or disadvantages. *African Journal of Hospitality, Tourism and Leisure* Vol. 4 (2)

[16] van der Ross, R. (2015). Identifying the benefits of social media within large financial institutions in South Africa. Department of Information Systems Faculty of Economic and Management Sciences University of the Western Cape.

[17] Zuckerman and Sauter, M. (2014). The coming swarm. Bloomsbury Academic.