African Journal of Inter/Multidisciplinary Studies 2022 | Volume 4(1): 64 -75 | DOI: https://doi.org/10.51415/ajims.v4i1.981

RESEARCH ARTICLE:

'We just want to be heard!' Dataveillance and Location Data – Do South Africans Care?

Sam Erevbenagie Usadolo[1], Bukelwa Belinda Mbinda[2] and Itumeleng Judith Maome[3]

Abstract

People's perceptions of digital communication platforms as related to dataveillance, and location data are examined in order to offer suggestions for increasing regulatory strength on the part of the government. Qualitative data collected from 65 participants through unstructured interviews were analysed. The analysis reveals that most of the participants are concerned about what the technology companies do with data collected without their consent. However, because of the numerous advantages digital platforms offer, they are not bothered about the technology companies' use of the data collected without their consent. The same applies to location data. Recommendations are offered that could help the South African government strengthen its regulatory framework.

Keywords: *Datafication; dataveillance; metadata; digital currency; location data*

Introduction

Datafication has grown as a new approach for understanding social behaviours (van Dijck 2014). This is thanks to the emergence of the Web 2.0 and its associated social network sites that have made it possible to characterise people's types of online social life on digital platforms. The characterisation takes into consideration people's relationships (distant and close relationships), interests, conversations, information searches, and political and religious expressions to make some predictive inferences about people's behaviours. Digital platforms in the form of social media provide a communication space for people to live out their social lives with minimal or no interference from gatekeepers. In addition, for many people, except for the data one needs to be connected online, the benefit of digital space or social media space seems almost free. For example, Facebook's free subscription has attracted billions of subscribers and has helped it to achieve its aims of turning the social activities of its subscribers such as "friending" and "liking" into algorithmic relations (Bucher 2012; Helmond and Gerlitz 2013). The same applies to Twitter, which has popularised people's online personas and created "followers" and "retweet" functions (Kwak *et al*. 2010).

The free-to-use social media platforms will continue to grow in leaps and bounds, especially in South Africa where there is a stifled and poisoned traditional media space that is generally not trusted (Garman and Malila 2016; Wasserman 2020). More important, the fact that social media literally provides a platform for voices that would have amounted to nothing in the traditional media space to be heard in their own languages and within their own sociocultural contexts will continue to make the platforms a convergence point for different views. In this light, Swart, Peters and Broersma (2018) observe that social media networks have influenced the media environment because subscribers choose them on their own terms and determine how they prefer to relate to others without restriction. However, the unrestrictive nature of the platforms encourages people to divulge information willingly or unknowingly to the social media establishments whose only

[1] Durban University of Technology, SamU@dut.ac.za
[2] Durban University of Technology, BukelwaM@dut.ac.za
[3] Durban University of Technology, judith@dut.ac.za

interest is to convert such information to what can only be described as *digital currency* because of what they gain from such conversions.

Put differently, the information shared on digital platforms is used by tech companies in the form of metadata to reach and classify their customers for targeted advertisements. The information trails left by subscribers when using digital platforms are manipulated by those with the technical expertise to achieve the primary objective of increasing the audience (or advertising) share and online purchases. All of this takes place without subscribers' expressed consent. The way people's information is used without their consent brings to the fore the issues of privacy and data protection. Recently, this debate has shifted from privacy in general to debates about data, and more specifically digital data (Owens 2019). Realising this, jurisdictions across the world have established privacy and data protection laws to safeguard and ensure individuality and autonomy in society. Consequently, there are ongoing policy debates about digital data (for example, the 'right to be forgotten' in Europe; see Kelly and Satola 2017), the White House review on Big Data (John 2014), the Australia Metadata Protection Law (Pearson 2019), and the South African Data Privacy Law or POPIA (National Law Review 2022). These laws and policies show privacy and data protection laws are proliferating and being adopted around the world.

The abovementioned laws are a response to protect individual privacy from being exploited by tech companies. However, as good as these measures are, that the individuals who use digital platforms have a responsibility to be mindful of the information they share online is posited. On this note, the extent to which people care about the collection of their data by digital tech companies is examined because such knowledge will not only assist with the creation of government policies regarding data protection but also provide a window to recommend a balanced regulatory framework that ensures digital tech companies operate fairly with respect to their subscribers. One of the ways this study engages with this phenomenon is to understand users' perceptions of these digital communication platforms as it relates to the dataveillance that is done by tech companies and the location data that are held by digital technology companies. In the next section, discussion of the extant literature is reviewed. This is followed by discussion of the method used in the study, the data analysis, and the findings and recommendations that will inform possible ways social media platforms can be regulated or checked.

Literature Review

Social media have become an important source of information for many people, and "they are considered to have unquestionably altered the nature of private and public communication" (Van Dijck, 2013: 7) due to the internet that has "become a great leveller of playing fields by bringing down the costs of connecting people to near zero" (Mäkelä 2019: 6). Although social media seems to be a free and convenient form of interpersonal relationships online, van Dijck (2014) warns that it is not free because the private information collected from tech companies' subscribers are metadata that serve as a form of currency that people use to pay for their communication services.

According to Manuel (2019):

> Metadata is the information recorded by the telco when you make a call or use the internet. It can include information such as where you are, whom you called or texted, how long you talked for, how frequently you called or texted someone, what services you used, what websites you visited and when, and much more besides.

With metadata, the technology companies can use people's information for their benefit. For example, the cell phones held by people are constantly giving off data as they move about carrying out their daily endeavours in cities, villages, and homes. The data are used for precise micro-targeting for marketing and political purposes (Valentino-DeVries 2019) after they have been analysed and categorised to obtain the core attributes of the people who own them. According to

van Dijck (2014: 200), metadata is a product of "digital trails left behind by people who live a considerable part of their life online". The "digital trail" gives huge amounts of information to the tech companies to determine a complete picture of their subscribers' activities or behaviour in different contexts.

Metadata also helps tech companies make their services better because they are able to establish peak calling times or locations that are popular on the network (Manuel 2019) as well as do dataveillance, a form of continuous surveillance through the use of metadata (Raley 2013) of their subscribers' activities. Furthermore, part of what comprises metadata is location data. Location data refers to personal information tracked to people's devices, such as cell phones, tablets, and suchlike, provided by social media networks, especially Google, to intelligence or law enforcement agencies about where you go, who your friends are, what you read, eat, and watch, etcetera. This information is put together as aggregated metadata for targeted advertising by social media companies, and sometimes, when compelled by law, mobile phone data of suspects accused of breaking the law are submitted to the court or intelligence agencies.

Google, which many people use, has a reputation for tracking cell phone users' locations for law enforcement agencies (Valentino-DeVrie 2019). The benefits of several Google apps have remained a bait for people to make location data history easy for Google to access. For example, Google prompts users to allow their location history for services like traffic alerts. Apart from big fishes such as Google and Facebook, smaller companies are also cashing in on subscribers' data. A medical appointment booking app (HealthEngine) in Australia was found to be sharing clients' personal information with lawyers who are interested in workplace injuries or vehicle accidents (Holloway 2019). In a nutshell, a growing phenomenon is tech companies using their subscribers' data for something other than what subscribers imagine. Scholars refer to this phenomenon as surveillance capitalism (Holloway 2019), a market-driven process where the commodity for sale is your personal data and the production of this data relies on mass surveillance of the internet.

The extent to which people's data are used by tech companies is raising increasing concerns. As such, instead of taking a regulatory route to protect online users, some are advocating that tech companies share their profits with online users. In other words, some activists are calling for what they refer to as 'data dividends' as compensation to people who divulge a significant amount of their personal data to tech companies without compensation (Kelly 2019). The concept of data dividends highlights issues that are likely to come up in the future about the data or information shared on online platforms by users. In other words, the concept of *datafication* is becoming a normal part of business and ordinary people's day-to-day activities. The issues are being discussed because of the increasing acceptance of datafication as a new social and organisational practice (van Dijck 2014). Datafication, as defined by Mayer-Schoenberger and Cukier (2013: 14), refers to the conversion "of social action into online quantified data, thus allowing for real-time tracking and predictive analysis". As such, both private and public agencies can lay their hands on increasing heaps of "metadata collected through social media and communication platforms, such as Facebook, Twitter, LinkedIn, Tumblr, iTunes, Skype, YouTube, and free e-mail services such as Gmail and Hotmail, in order to track information on human behaviours" (van Dijck 2014: 198).

The tech companies are subject to applicable laws and regulations in the jurisdictions in which they operate, and this may be one of the reasons subscribers to their services have faith in the collection of their (meta)data. However, evidence abounds that this, in many cases, is not true. For example, an app developed by the Australian government to track people's social contacts that will help to fight COVID-19 received lukewarm acceptance by the public when launched because of the fear that it will be used to spy on them. There are also stories in South Africa where people's data have been used for purposes for which they did not sign up. For example, information provided by MTN, Vodacom, Cell C and Telkom revealed that security agencies are using information on their networks to spy on people's numbers every year (Business Tech 2017; Hunter 2020). Privacy concerns raise a great many issues as well as a need for examining the phenomena of dataveillance

in greater depth. Finding out people's views about their personal data that are held by tech companies is the aim of this research.

Method

The population for this study is middle- and low-income South Africans in the Eastern Cape Province. The middle-income participants in this study were teachers, nurses, and government department workers with at least a university degree. The low-income participants were frontline staff members in both primary and secondary schools, such as cleaners and kitchen staff and frontline staff in hospitals in the Eastern Cape. Most of the low-income participants had achieved Grade 12 or less qualifications.

A total of 65 participants between 20 and 58 years who were purposively selected took part in this study. The participants' average age was 30 years. The sample of participants was 65% females and 35% males. One of the criteria used to select the participants was that they had been active social media users for the past three years and have more than two social media accounts. These accounts could be any of the following: Facebook, Twitter, Instagram, and Skype, among others. They were also using smartphones. It was very easy for the participants selected to meet these criteria, and they all claimed to be active social media users for several reasons, including connecting with both old and new friends, online dating, accessing current news, employment-related purposes, etcetera. Their join-by dates on their profiles, which the participants showed to the researcher, were used to verify the criteria of being active social media subscribers for at least three years. Those who did not meet the criteria were excluded.

Data for the current study were gathered through 40 – 45-minute interviews with each of the participants who were assisted by one research assistant. The research assistant was an honours degree student at a nearby university and was trained as a research assistant in the study. Interviews consisted of unstructured conversations with the participants that were audio-recorded and transcribed. According to Borg (2006) and Corbin and Morse (2003), an interview is a verbal encounter with participants in a research context; it is considered a more appropriate means of collecting data and examining perceptual phenomena than other methods. The main objective of the study was to find out the participants' perceptions about what the social media platforms' owners do with the information they knowingly and unknowingly divulge while using social media. The demographic information of the participants was collected in preliminary meetings prior to the interview process.

A significant percentage of the participants were interviewed in their workplaces during their breaks, and a few were interviewed after work in the evening. Because the interviews were audio-recorded, pseudonyms were used to identify the participants during the interviews. Consent forms were given to the participants to read and sign. This was after the purpose of the study was explained again in addition to what the participants were told in the preliminary meetings. Participants were told the study was anonymous and that they could withdraw from the study at any time. In addition, participants were told to seek clarity about any questions asked that were not clear to them during the interview process. Following the unstructured interview approach, participants were allowed to provide further information in addition to the responses they had given, which allowed them to delve deeper into what they felt were appropriate responses. At the conclusion of the interviews, participants were given R30 recharge voucher as a reward for participating in the study.

The questions put to the participants were:

i. Were they bothered or concerned about social media's (Facebook Twitter, etc) use of information about them?
ii. Had they ever changed their use of social media (Facebook, Twitter, etc.) privacy settings in response to these concerns?

iii. What kinds of personal information would they not want internet companies like Facebook or apps to access or use?

Audio-recorded transcripts were checked to ascertain their accuracy by the researcher and research assistant. Data analysis was guided by the framework analysis approach as explained by Srivastava and Thomson (2009) and Krueger and Casey (2000). The framework analysis approach is appropriate for analysing data collected through interviews because it allows a researcher to either analyse data during the collection process or after the data has been collected (Srivastava and Thomson, 2009). Thus, the analysis went through the five-step process suggested by Ritchie and Spencer (1994), these steps being familiarising, identifying a thematic framework, indexing, charting, and mapping the interpretation.

As per the five-step process, the analysis went through a process of identification and reporting patterns (themes) within the data. Organising and transcribing the interviews were followed by going through each individual participant's interview data systematically and identifying codes in the form of labelling words and phrases. To make reporting of the data easy, these descriptive codes were put together to extract the themes used in the discussion of the findings. Findings in this study are discussed below as they relate to five themes used to organise the participants' responses. To ensure the anonymity of the participants and for ease of analysis and discussion, unique identifiers were used for participants. For example, P1 stands for Participant 1 and P2 for Participant 2, and this continued with the mention of participants whose findings are referred to during the course of the analysis. The participants' comments that best represent the essence of what other participants conveyed are used in the analysis. The data are analysed below according to the identified themes that reflect the participants' views.

It's all about Keeping the Network Alive and Relevant

Dataveillance and what location data of participants are used for is not important to most participants because the key reason for their social media presence is to connect with family and friends, especially being able to find old friends and reconnect with them, as well as maintain current relationships. Most of the older participants (between 35 and 58 years) commented that using Facebook, Instagram, Signal and Twitter was their best way of knowing about their children who are not staying with them.

P1 commented as follows:

> The only thing that has kept me there is because my kids, and friends are likely to be there, and I just want to see what they are doing and who they are hanging around with. Dataveillance or whatever it is called is not an issue to me. It is the government responsibility to make sure there is a reconnaissance of people's chatters online. We discuss the government itself. Doesn't the government have a responsibility to see that the chatters about them is true and take down untruth? In other words, is social media helping people to peddle anti-government views? If they check, they will know.

These comments squarely laid the surveillance or investigation to weed out "untruth" in the lap of the government. Social media is porous, and anything and all things given to it stay on it and go through it to other sources. Hence, the suggestion is that the government should police what happens on the platforms. In the context of this study, it means the government should sanitise the operation of the platforms so that information disseminated on the platforms is what people can proudly claim as theirs. In doing this, the government can also make sure people's data are not used without their permission because if they do not permit the platforms to use the data outside of the original purposes, it means they would not proudly own up to it when the chips are down about their data.

Although social media is an important tool to support social interactions in a world in which people are dispersed and physically separated from friends and family, the question of dataveillance and

location data means nothing to the participant, and others held similar views. A minority of participants (*N*=12) also talked about not liking the feeling that they are being watched and the possibility that their personal information is being accessed or bank details stolen. However, these issues were not considered serious enough for them to be worried about their activities on social media platforms or to have a view about who should be making sure people's data are not used for purposes for which the platforms' subscribers did not sign up.

Projection of Voice and Participation in Social Issues

As much as 65% of the participants said they did not care about what social media platform owners and internet companies do with their data. The common reason stated was that social media allows them to have unfettered access to and participation in socio-political issues.

According to P2:

> The benefits outweigh the commercialisation and spying thing you are talking about. I can comment on social and political issues because of social media.

P3 said that:

> What is good is also having a disadvantage. I participate in many things with the help of social media. It reduces face-to-face contact … so the question of transportation cost for a meeting is reduced.

In addition to the above, P4 said,

> Did I and many others like me exist in this South Africa before Facebook, Instagram, and Twitter? Tell me? Simple … let them go with information they get from me. I am happy they target me with an advert … it means I'm important, and are they going to force me to buy their products? This thing of intelligence doesn't bother me.

These three participants' (P2, P3 and P4) responses represent as much as 65% of the participants who emphasized the advantages of online platforms: social media platforms give them the opportunity to project their voices in day-to-day socio-political issues, which is in sharp contrast to the traditional media in South Africa and suggested that the question of dataveillance and location data are not very important. With online platforms, the question of a gatekeeper barely exists as long as the material posted does not hint towards terrorist intentions and/or is hate related, which some online platforms would remove a few minutes after they surface online. However, many male participants whose use of social media is for participating in socio-political issues said they would delete their social media accounts if they had evidence that their information was being used without their consent. P5's views reflect what others in this group mentioned:

> I have heard that the technology companies use our data for their business; they sell our information and all sort of things, but I do not have evidence. So, I cannot act on something I cannot prove. If I know they use my information, the minute I know, I will delete my account. Why will I allow a snitch on my online space?

In addition to P5's response, P6 stated that he relished the fact that social media gives him a voice and a platform to contribute to social issues, "but if the cost is for me to do away with my privacy, I will do away with social media by the time it is patently clear to me that issues about my privacy are [on a] perilous trajectory". P6 seems to have taken another look at the question of data privacy based on further pertinent questions asked. P6 is ready to act if his privacy is threatened.

Poor Knowledge about what Online Platforms do with Metadata

Most people were unsure about how Facebook and other social network platforms use their personal information besides advertising. For example, very few were aware of the Cambridge Analytica scandal or how, through the use of an algorithm, their metadata are aggregated and then used for targeted advertisements or to make political decisions about them. Even when they did refer to these issues, they had difficulty explaining how personal data were involved. P7, whose views summarize what other participants said, commented as follows:

> Well, I know Facebook collected the data for that Cambridge business, and they collected it via a quiz with an app, and then passed it on to other parties. So, I think that's all they do. I think it's just maybe for them to earn money off it. I don't really know. And bad people will be bad people … it does bother me, but not at the expense of my continuous usage of social media such as Facebook. Facebook will be Facebook – it will continue to operate and outlive most of us.

The permanency of Facebook is highlighted in P7's response with respect to different products that make it appeal to subscribers. This suggests people will continue to use Facebook even if people's information is passed on to third parties. P7 had no view about whose responsibility is it to regulate the social media even when the question was asked directly. His response to the question was that Facebook will outlive everyone, and it will continue to serve its subscribers even in the face of tough regulation. This suggests that there is no need to regulate Facebook because regulation would not achieve anything. In addition to the previously analysed data, P6's response shows a lack of understanding of what online platforms use subscribers' metadata and what regulation is needed to stop the abuse of people's metadata. P8 was particularly blunt about claiming zero knowledge about what his metadata represent to digital platforms. He said:

> Honestly, I don't know anything about data or how my information online can be used. I always see some websites requesting that I allow my location to be used, but what that means is just being realised because you are explaining it now. I think these internet companies are doing a bad thing. For now, I don't have a choice; I will maintain engagement with people on the social media platforms I currently subscribe to.

Even when the participants were told about the choices they could make to safeguard their information or that they could quit social media platforms completely because of privacy concerns, from P7 and P8s' responses, it seemed they have concluded that there is nothing they can do to protect their information online or from the unauthorised use of their information by social media platforms because 'bad people will be bad people' (P7), so there is nothing that can be done, and '… internet companies are doing bad thing' (P8). P7 acknowledges that telecommunication companies monetize their subscribers' metadata.

This is about Everyone's Business Online

For most of the participants, social media enables them to sell their products and tell their stories about their products the way they want. With social media, they are their own PR and communication strategists. A significant percentage of the participants said for these reasons, 'snitching' and 'manipulation' done by the social media companies are worrying but not enough to give them sleepless nights.

P9 reflected the views of other participants interviewed:

> My friend, do you know how much it costs to advertise a product in a newspaper or TV? Where do you think somebody from my socio-economic

> background will get the money? This internet of things is good for my business. I am my own business strategist, and my clients understand me. I don't even think of all these [things] you are saying. It is for the government to worry about because my story is their story.

P9 believes that whatever is being discussed on social platforms is dictated by what is currently happening at all tiers of government. It is therefore the responsibility of the government to have a regulatory framework in place that will make sure people do not misrepresent government discourse about events. In summary, the findings show that majority of the participants do care about the privacy and security of their personal information; however, they do not care enough to feel worried or stop using social media platforms. It is for the government's responsibility to feel worried so that they are not misrepresented.

It is not Spying or Social Media Gain that is our Problem

Most of the participants whose comments fall under this theme were worried to learn that their information could be used for something other than what they had intended it to be used on social media. Some were terrified that location data could tell a great deal about where they have been and who could have been with them, and this could be used by law enforcement agents if there is a need. Three of the participants whose views summarise others' views are reported. P10 noted as follows:

> This surveillance or spying you mentioned is very worrying to me. Knowing what they do with our information is worrying, but this is not our immediate problem – what is our problem is what you have not mentioned. Look, I believe some of the staff members of the social media thing use the information to cyberstalk us – this is what you have not mentioned. You should tell the government to stop this. Yes, thank you. This is where regulation should address.

P10 is clearly rattled about knowing the degree to which the information trails social media subscribers leave on their social media platforms can be used by social media companies but like other participants will continue to use social media. However, he is concerned about cyberstalking, which he believed is being done by employees of social media companies. He would therefore prefer that there is a regulation against cyberstalking. Other participants are not worried about cyberstalking but the general abuse of their information. As explained P11,

> White monopoly capital will do anything and get away with it. Why would they collect my information for an advert or what do you call it … cold-calling? They are wrong. I didn't sign for my information to be used for these things you mentioned or for my location to be monitored. This government is quiet. Are they not aware? The government must stop it. I hear of some laws they made recently regarding this internet thing. I hope this law is strong. It is not me who will stop using social media. Everybody wants a voice; we just want to be heard.

The 'some laws' P11 is referring to is the recent POPIA Act in South Africa that is meant to prevent abuse and unlawful use of people's information. To P11, the social media platforms can only be owned by White South African businesspeople who are referred to as White monopoly capital. He said he did not have the intention of quitting social media because it is the duty of the government to regulate what the social media platforms owners do with people's information.

P13 said she has been trying to remain private or careful about her personal information online:

> To some extent, you can control how your information is seen and used online. I do this, and I rarely share information I am not comfortable with others

> knowing it. The other side of your story about location data is frightening because if an app wants to know your location, and you say no, the app may not work properly, or you may not be able to install the app on your devices. I have been a subscriber to different platforms of social media and for what they do to me in terms of social issues, I can't see myself quitting them. So, it is the responsibility of the government to ensure that these social media platforms are safe for people to use.

The common view with respect to this theme is that the government has a responsibility to protect South Africans against the abuse of people's information. There is, therefore, no need to worry about when the government is doing its work appropriately.

Discussion and Recommendations

The aim of this study was to examine the views of participants about dataveillance and location data. The responses from the participants were varied, but they agreed that social media and the internet generally were central to their day-to-day activities and did not see themselves quitting social media platforms. In general, they are less bothered with how their data are used by telecommunication companies. The participants' relationships with their social media platforms are according to Dhaenens and Mollen (2017: 25-26) described as social media *pervasiveness,* which refers to the growing "ubiquity, embeddedness of and reliance on digital software-based media in people's everyday life, requiring them to display and adopt complex and differentiated ways of handling and managing their engagement with media". If the findings are extrapolated to represent the general population of subscribers' using social media, it means that the overriding concerns are the advantages derived from their use of the internet and their use of the social media platforms. Such concerns trump all other concerns, such as insults from other users and what the social media platforms do with people's data.

Based on the gist of the findings, many participants do not believe it is their duty to hold the technology companies to account or to independently be reticent about the information they share online. Hence, according to Ong and Das (2019), it is duty of the digital platforms' owners not to abuse subscribers' metadata. As explained in the literature review, the current business model of the telecommunication companies and platform owners allow them to take undue advantage of their subscribers, and they are unlikely to self-regulate against their business interests. What is necessary to regulate the social media platform beyond the existing regulations that allow them to use subscribers' data purely on their own terms? The participants revealed in their responses that they believe the government needs to have more regulatory muscle than they currently have to check what social media or digital platforms do with people's data.

To do this, the government needs to let telecommunication companies know that they are publishers and should be guided by regulations and ethics (Lidberg 2019) to which the mainstream media are subjected. Given evidence of abuse such as cyberstalking, abuse of subscribers' information and unauthorised use of people's demographic details for marketing purposes, the participants' recommendation that the government should rein in social media tech companies appears justified. In this regard, it is very necessary for the government to develop a policy that monetises people's metadata use for the general good of the country or the people whose data have been used. This is important because when the telecommunication companies know they will be asked to pay for the use of their subscribers' metadata, they are most likely to stop the brazen way metadata are misused or used without subscribers' consent.

The findings in this study have shown that social media has a great many advantages for participants, and the advantages have strengthened their continuous presence on social media. Similar to the participants in this study, social media subscribers in other countries believe that it is the prerogative of social media to self-regulate, for example, to reduce hate speech, cyberstalking, etcetera. For example, following the daily harassment and bullying a Philippine journalist (Maria

Ressa) suffered, she suggests regulation that ensures accountability and liability on the part of the platform owners as one of the fundamental changes required (Posseti *et al*. 2021). In the context of the data analysed, the South African government needs to establish a regulatory framework that clearly spells out the accountability and liability measures that stem from the misuse of people's information by technology companies. This should be complemented by investing in tools that educate people about online platforms. For example, an Instagram tool such as *Restrict* should apply to other platforms to dissuade unacceptable conduct on online platforms.

As the analysed data have shown, there are many concerns about what content on social media is being monetised and who benefits (Berg, Morton and Poblet 2021). For this reason, there should be regulations that let subscribers know what their information is worth so that they can decide where to share such information.

Conclusion

Despite the enormous benefits the technology companies derive from the unauthorised and surreptitious use of their subscribers' information, the data analysed and discussed show that revelation of such benefits is not enough to dissuade people from digital platforms. The reason is that the benefit of what they get in their participation online far outweighs any other consideration especially to those who use their online presence to connect and market their products. Another major reason is the unfettered presence and voice that social media is giving to a section of the society that was voiceless or unheard before the advent of social media. What is clear from the responses given by the participants is that they believe the responsibility for the regulation of social media lies with the government and the social media companies and not with social media participants because participants will continue to use social media platforms for their benefits. While there are regulations in many jurisdictions across the world regarding the excesses of big technology companies, perhaps the suggestion that people's metadata be monetised for the general good of the country will help. In addition, the discussion, and recommendations above point to the directions that need to be taken by regulatory bodies in South Africa to prevent unauthorised use and abuse of South Africans' metadata.

References

Berg, C., Morton, E. and Poblet, M. 2021. Social media has huge problems with free speech and moderation. Could decentralised platforms fix this? Available: https://theconversation.com/social-media-has-huge-problems-with-free-speech-and-moderation-could-decentralised-platforms-fix-this-157053 (Accessed 16 March 2021).

Borg, S. 2006. *Teacher Cognition and Language Education: Research and Practice*. London: Continuum.

Bucher, T. 2012. Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. *New Media and Society*, 14(7): 1164–1180.

Business Tech. 2017. Cops are 'spying' on over 70,000 Vodacom, MTN, Telkom and Cell C customers each year. Available: https://businesstech.co.za/news/mobile/194092/cops-are-spying-on-over-70000-vodacom-mtn-telkom-and-cell-c-customers-each-year/ (Accessed 20 September 2017).

Corbin, J. and Morse, J. M. 2003. The unstructured interactive interview: Issues of reciprocity and risks when dealing with sensitive topics. *Qualitative Inquiry,* 9(3): 335–354.

Dhaenens, F. and Mollen, A. 2017. Coping with intrusive media. In: Das, R. and Ytre-Arne, B. eds. *Audiences, Towards 2030: Priorities for Audience Analysis.* Surrey: CEDAR, 25-27.

Funnel, A. 2020. It's Trump vs Biden in the US presidential race, and digital strategy matters more than ever. Available: https://www.abc.net.au/news/2020-04-12/trump-biden-us-presdential-election-social-media-data-ads/12070244 (Accessed 10 April 2020).

Garman, A. and Malila, V. 2016. How South Africa's media deny the country's youth a voice. Available: https://theconversation.com/how-south-africas-media-deny-the-countrys-youth-a-voice-54853 (Accessed 20 September 2017).

Helmond, A. and C. Gerlitz. 2013. The like economy: Social buttons and the data-intensive web. *New Media and Society*, 15(18): 1348–1365.

Holloway, D. 2019. What is surveillance capitalism and how does it shape our economy? The Conversation. Available: https://theconversation.com/explainer-what-is-surveillance-capitalism-and-how-does-it-shape-our-economy-119158 (Accessed 20 August 2019).

Hunter, M. 2020. Cops and call records: policing and metadata privacy in South Africa. Available: https://www.researchgate.net/publication/342078824_Cops_and_call_records_Policing_and_metadata_privacy_in_South_Africa (Accessed 12 February 2021).

John, P. 2014. Findings of the big data and privacy working group review. Available: https://obamawhitehouse.archives.gov/blog/2014/05/01/findings-big-data-and-privacy-working-group-review (Accessed 11 June 2020).

Kelly, H. 2019. Companies use your data to make money: California thinks you should get paid. Available: https://edition.cnn.com/2019/02/13/tech/digital-dividend-california/index.html (Accessed 14 February 2019).

Kelly, M. J. and Satola, D. 2017. Right to be forgotten. Available: https://ssm.com/abstract=2965685 (Accessed 25 December 2020).

Kwak, H., Lee, C., Park, H. and Moon, S. 2010. What is Twitter, a social network or a news media? Available: http://an.kaist.ac.kr/traces/WWW2010.html (Accessed 12 June 2021).

Krueger, R. A. and Casey, M. A. 2000. *Focus Groups: A Practical Guide for Applied Researchers.* Thousand Oaks, CA: Sage.

Lidberg, J. 2019. Twitter is banning political ads – but the real battle for democracy is with Facebook and Google. Available: https://theconversation.com/twitter-is-banning-political-ads-but-the-real-battle-for-democracy-is-with-facebook-and-google-126260?utm (Accessed 8 December 2019).

Mäkelä, A. 2019. Social media for change: Ideas, tools and best practices for civic engagement and elections. Available: https://www.citizensforeurope.eu/learn/social-media-for-change-ideas-tools-and-best-practices-for-civic-engagement-and-elections (Accessed 10 January 2020).

Manuel, D. 2019. Think your metadata is only visible to national security agencies? Think again. Available: https://theconversation.com/think-your-metadata-is-only-visible-to-national-security-agencies-think-again-121253. (Accessed 6 August 2019) (Accessed 11 January 2021).

Mayer-Schoenberger, V. and Cukier, K. 2013. *Big Data: A Revolution that will Transform how we Live, Work, and Think*. London: John Murray Publishers.

National Law Review. 2022. South Africa's protection of personal information act. Available: https://www.natlawreview.com/article/south-africa-s-protection-personal-information-act-2013-goes-effect-july-1 (Accessed 16 January 2022).

Ong, J. C. and Das, R. 2019. Two concepts from television audience research in times of datafication and disinformation: Looking back to look forward. In: Shimpach, S. ed. *Routledge Companion to Global Television*. London: Routledge, 20-32.

Owens, J. 2018. The debate around data privacy is missing the point. Available: https://towardsdatascience.com/the-debate-around-data-privacy-is-missing-the-point-1fcdc4effa40 (Accessed 7 April 2020).

Pearson, M. 2019. Australian metadata laws put confidential interviews at risk, with no protections for research. Available: https://theconversation.com/australian-metadata-laws-put-confidential-interviews-at-risk-with-no-protections-for-research-121320 (Accessed 7 October 2020).

Possetti, J., Maynard, D., Bontcheva, K., Hapal, D. K. and Salcedo, D. 2021. *Maria Ressa: Fighting an Onslaught of Online Violence*. Washington, D.C.: International Centre for Journalists.

Raley, R. 2013. Dataveillance and Countervailance. In: L. Gitelman, ed. *'Raw Data' is an Oxymoron.* Cambridge, MA: MIT Press, 121–146.

Ritchie, J. and Spencer, L. 1994. Qualitative data analysis for applied policy research. In: Bryman, A. and Burgess, R. G. eds. *Analyzing qualitative data*. London: Routledge, 173–194.

Srivastava, A. and Thomson, S. B. 2009. Framework analysis: A qualitative methodology for applied policy research. *Journal of Administration and Governance*, 4(2): 72–79.

Swart, J., Peters, C. and Broersma, M. 2018. Shedding light on the dark social: The connective role of news and journalism in social media communities. *New Media and Society*, 20(11): 1–17.

Valentino-DeVries, J. 2019. Tracking phones, Google is a dragnet for the police. Available: https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html?smid=nytcore-ios-share (Accessed 14 May 2019).

Van Dijck, J. 2013. *The Culture of Connectivity: A Critical History of Social Media*. New York: Oxford University Press.

van Dijck, J. 2014. Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance and Society,* 12(2): 197–208.

Wasserman, H. 2020. The state of South African media: A space to contest democracy. *Publizistik*, 65: 451–465.