*SACJ* 35(2) December 2023
Research Article

# Online Platform Privacy Policies: An Exploration of Users' Perceptions, Attitudes and Behaviours Online

Kimberley Mugadza, Gwamaka Mwalemba

University of Cape Town, Private Bag X3 Rondebosch, Cape Town, 7701

**ABSTRACT**

In January 2021, Meta (then Facebook) published an update to its WhatsApp privacy policy which included, among other things, a decision to share some user data with Facebook. This action, together with previous events like the notorious Cambridge-Analytica data breach, has sparked debates about the protection of online privacy, specifically the balance of rights and responsibilities relevant to the protection of social media user data. This qualitative study contributes to that debate by exploring the perceptions and reactions of South African WhatsApp users to these policy changes. The findings highlight the significance of platforms like WhatsApp in the daily socio-economic activities of users in developing countries. This reliance on social media for communication and access to vital information creates an imbalance of power between users and platform owners. The situation is worsened by the lack of effective regulatory frameworks that governments and institutions in developing countries can use to enforce their privacy laws, leaving users vulnerable to potential exploitation from digital platforms. This study contributes to the broader discourse on safeguarding online privacy as Western technology companies continue to gain access to data that is generated by an ever-increasing global user base.

**Keywords** social media, online privacy, consumer behaviour, WhatsApp

**Categories** • **Information Systems** ∼ **Information systems applications, Collaborative and social computing systems and tools, Social networking sites** • **Social and Professional Topics** ∼ **Computing/technology policy, Privacy Policies**

**Email**
Kimberley Mugadza – mgdkim001@myuct.ac.za,
Gwamaka Mwalemba – gt.mwalemba@uct.ac.za (CORRESPONDING)

**Article history**
Received: 29 January 2023
Accepted: 2 November 2023
Online: 14 December 2023

## 1 INTRODUCTION

A person's digital presence is expanding continuously as more aspects of our daily lives migrate online, particularly onto social media. The rise of social networking sites (SNSs) has changed the way in which people communicate and conduct business on a global scale (Abbas Naqvi et al., 2020). Not only have SNSs become the predominant online platforms for marketing and networking, they have also become widely viewed as the most useful, cost-effective, and popular internet technology tool for reaching consumers (Duggan et al., 2015). As presented by

Mugadza, K., and Mwalemba, G. (2023). Online Platform Privacy Policies: An Exploration of Users' Perceptions, Attitudes and Behaviours Online . *South African Computer Journal* 35(2), 78–96. https://doi.org/10.18489/sacj.v35i2.17443


*SACJ* is a publication of *SAICSIT*. ISSN 1015-7999 (print) ISSN 2313-7835 (online)

Perrin (2015), SNSs were initially perceived as a simple and functional way for people to build professional networks online. SNSs have evolved since then as companies recognised opportunities for commercialisation. There is now no single definition of what qualifies as an SNS, but it is loosely defined as a community on an online platform that sees users with common interests and needs sharing information, improving productivity, exchanging news and insights, and maintaining a multichannel platform for the retailing of goods and services (Hashimzade et al., 2014). With the use of familiar, convenient, and user-friendly interfaces, people now prefer to use SNSs as their primary means of communication.

The most used social media applications have now become applications like WhatsApp that allow users to send real-time text and multimedia messages to their peers at no cost (Church & de Oliveira, 2013). These types of applications have become the most common social media platforms of the 21st century due to their convenience. However, it must be noted that one of the most prominent issues arising from using these types of applications is that users are exposed to large volumes of unregulated messages or information (Ahad & Lim, 2014; Nobre et al., 2022). Data from a study conducted by Montag et al. (2015) showed that the use of WhatsApp accounted for 19,83% of all smartphone behaviour. This was compared to Facebook usage at the time, which amounted to 9.38%.

In recent years, several privacy-related debates and events have been covered extensively in the media. Many of these events were related to companies with a significant influence over the information technology (IT) industry such as Facebook and Google (Fiesler & Hallinan, 2018). Due to these recurring privacy-related events and the widespread consumption of social media and digital content, technology designers and policymakers are now obliged to remain more accountable to their users. Consequently, these policymakers and designers are now faced with the challenge of balancing out their users' unpredictable privacy habits with regulations and guidelines regarding the personal data collected from them (Compañó & Lusoli, 2010).

When WhatsApp introduced its new privacy policy on the 4th of January 2021, users would have seen the changes appear as a pop-up message when they opened the application. This policy was introduced after WhatsApp's latest update, at the time, which required users to consent to have some of their data on the app linked to Facebook by no later than the 15th of May 2021 (Wijoyo et al., 2021). Because of this, WhatsApp received criticism from its users, with some considering closing their accounts and migrating to similar messenger apps like Telegram and Signal (Wijoyo et al., 2021). This decision, however, was not simple because WhatsApp has become a central point of communication for many users, with many activities, like sharing resources for online learning, being carried out on the platform during the pandemic.

The event has also been linked to a similar online privacy breach, namely the 2018 data breach with Facebook and Cambridge Analytica, which became one of the most publicised data breaches in recent years. This is because a swathe of individuals had data about them collected without their consent (Cadwalladr, 2018). The scale of data misuse, combined with the alleged claims of mass manipulation, provoked users and resulted in several protests which

called for people to close their Facebook accounts.

Since it entered the South African market, WhatsApp has been one of the key drivers in narrowing the divide between urban and rural areas in terms of internet engagement (Shambare, 2014). Overall, WhatsApp usage in South Africa increased by 40% during the lockdown in 2020, with more people using the app to stay connected with family members, friends, and colleagues (Parez, 2020). WhatsApp is no longer a simple instant messenger that can be used for social purposes; it has now become a central part of communication for many South Africans' lives as matters relating to school, work and business are now discussed more frequently over the app (Parez, 2020). Furthermore, WhatsApp was already a central platform of communication for South Africans before the pandemic. The circumstances brought about by the COVID-19 pandemic have only heightened WhatsApp's relevance in South African society as more aspects of people's lives, such as school and work, migrated online. Thus, because of their dependency on WhatsApp services, South African users received WhatsApp's proposed privacy policy with some resistance (Fiesler & Hallinan, 2018).

When WhatsApp was bought by Facebook in 2014, users were reassured that there were no plans to share their data with third parties or any other platform. However, the supposed change in stance shown by the introduction of the policy, Facebook, Cambridge Analytica, and similar privacy policy events have thus led to undermined trust amongst users and a perception that corporations are prioritising profit over user well-being (Bhattacharjee & Dana, 2017). WhatsApp also received criticism about its policy due to its bias. For instance, users in select European countries were exempt from the new policy. Meanwhile, users in other countries, particularly those in developing countries like India and South Africa, were not given the same option (Rajpurohit & Yadav, 2021), as refusing to accept the new terms meant that one's account would be fully discontinued. This limited users' autonomy regarding their decision over this policy. Incidents like these have also led to debates about the ethical standards of individuals' privacy and data security online as individuals and organisations deal with the increasing risk of online security threats and privacy in an increasingly digitised environment (Hinds et al., 2020). Therefore, it becomes essential to understand how social media users understand, perceive, and react to issues related to online privacy.

This study is an extension of a publication that explored how WhatsApp users based in South Africa perceived the January 2021 policy changes and how these views influenced their reactions to the policy (Mugadza & Mwalemba, 2022). This paper adds to the findings from the previous article and aims to explore the reasons behind users' actions on social media platforms. It does so by attempting to answer the following research question:

*"How do WhatsApp users in South Africa view their role in ensuring their online privacy?"*

The next section highlights several key research topics related to online privacy and social media. This is followed by a brief description of how the study was designed and conducted. The key insights found from the data are then presented and discussed, followed by a brief conclusion.

https://doi.org/10.18489/sacj.v35i2.17443

# 2 BACKGROUND

## 2.1 Social Media and Online Privacy

The use of social media can be empowering for users because SNSs seemingly offer their users creative control over the representations of their identities online (Bonanno, 2014). However, online users also generate large volumes of data, which companies rely on to improve their services for their customers and users. Hence, it is becoming a requirement for users to consent in some form to have their data shared with either the SNS service provider or another third party. This has implications for overall user privacy, autonomy, and empowerment (Beigi, 2018).

However, despite the concerns related to online privacy for users, Gibbs et al. (2010) argue that the benefits of having an online presence outweigh its risks. For instance, sharing one's data helps users and businesses maintain a relationship that can be used to personalise services based on an individual's preferences (Krasnova et al., 2010). This improves a business's operational efficiency while increasing user experience for its users or customers. There are, however, some risks that must be noted. As a result of the increased privacy concerns, people are becoming more concerned about their online presence and privacy and are particularly worried about the possible misuse of their data (Baruh et al., 2017). Consequently, users on the internet are becoming more vocal about their desire to have more control over their personal information online (Smit et al., 2014).

Having access to online privacy means that people have the freedom to determine when, how and to what extent information about them is shared with others (Smyth, 2014). As companies collect, use, and share the user data that is available online, people often lose control over their personal data. Hence, one of the most significant challenges faced by users who are active on the internet relates to their privacy online. This challenge is faced to the extent that managing and protecting one's online presence has become an essential part of daily life (Boerman et al., 2018).

## 2.2 Privacy Actives

A survey was conducted in 2019 by Cisco, an American technological conglomerate, to examine the actions and attitudes of adult online users regarding their data privacy. Results from the survey revealed that 32% of respondents identified themselves as individuals who care about their data security and privacy online (Redman & Waitman, 2020). Not only were these individuals willing to be proactive about ensuring their privacy, they had also already done so by switching companies or service providers over data-sharing policy disputes (Redman & Waitman, 2020). Individuals who fall into this category have since become known as "privacy actives", with 90% identified from the sample population believing that the way their data is used reflects how they will be treated. Based on these results, it was concluded that privacy actives are, therefore, unlikely to interact with a social media platform, application and (or) business if they do not trust how their data is going to be used (Redman & Waitman, 2020).

https://doi.org/10.18489/sacj.v35i2.17443

When asked whether they felt that they could protect their privacy online sufficiently, 52% of non-privacy actives agreed. Only a third (33%) of privacy actives agreed. The main concern raised by users was that it is not easy to know exactly how or when their data is or is going to be used. In other words, it is not easy to assess the trade-offs of using resources like social media applications upfront because one cannot know the purposes for which data will be used (Redman & Waitman, 2020). The survey results also revealed that privacy actives are the most likely to read privacy policies, where 83% actively do. However, the consensus within the sample population was that the language used in these policies could be unclear to the average person. Respondents also stated that having a detailed privacy policy or terms of use page is helpful, but taking the time to sort through it can be impractical due to its length and time constraints (Redman & Waitman, 2020).

## 2.3 Online Privacy vs. Convenience

Social media users and online consumers value their safety and want to feel safe (Goldstuck, 2012). Putting this into practice, however, is not something the average person finds practical. More than 80% of the individuals who participated in the Cisco survey felt that they could not protect their data and privacy online. This implies that users expect more of the responsibility for their data to be that of service providers like WhatsApp (Shillair et al., 2015).

Contrary to the results from the Cisco study (Redman & Waitman, 2020), prior research (Acquisti & Gross, 2006) showed that when forced to choose, users are more likely to opt for convenience over privacy. This behavioural pattern was observed even in users who ranked their privacy concerns higher than other societal concerns like politics (Schreiner & Hess, 2015). Additionally, results from a similar study (Stieger et al., 2013) revealed that users generally view the perceived benefits of using social media as a sufficient incentive to trade their privacy at the cost of their convenience.

A study was conducted by Schreiner and Hess (2015) that explored whether users would be willing to switch from one service to another over privacy concerns. It was found that dissatisfaction with privacy practices has a more substantial effect in influencing users to discontinue their use of a service over the attractiveness of a sound privacy policy (Schreiner & Hess, 2015). However, despite this observation, the authors also observed that it is more common for users to be unwilling to switch services. The authors attributed this to the high social cost and inconvenience that users would incur when restructuring their central networking platforms. In other words, though they express concern about their online privacy, users are unlikely to reflect their concerns in their actions (Acquisti & Gross, 2006).

There is, however, also some evidence to suggest that users can be willing to change their behaviour in some form after an online privacy breach, even if their behaviour does not reflect their concerns (Budak et al., 2021). This behaviour can be described as user resilience, where perceptions of past events influence how lenient users are when similar incidents occur in the future. This is because a user's online activity in various dimensions is supposedly affected by an online privacy violation event. The user's perceptions of the stressor (i.e., the social media

platform) are also likely to shift after the privacy breach has occurred (Budak et al., 2021).

When consumers (users) are affected by a stressor like an online privacy breach, they are likely to respond to this event with resistance. The level of resistance is likely to be influenced by their knowledge about, perceptions of, and attitudes towards a similar event. Their perceptions can be described as what users think about the event (Compañó & Lusoli, 2010). Their attitudes would refer to their beliefs about the event, and these are derived from the opinions (perceptions) that they would have formed about the event. Lastly, their behaviours can be described as how the users would react to events based on their opinions and beliefs. This can apply to how they would conduct themselves under normal circumstances or how they would respond to triggered events. This is described in the diagram in Figure 1 as the antecedents that influence an individual's level of resistance (Budak et al., 2021). Users' reactions to an online privacy breach can also be influenced by micro and macro-economic factors such as their educational and professional background, age, level of income, individual attitudes towards internet usage and cultural influences. The combined impact of all these factors will therefore influence how users are likely to respond to an online privacy violation or similar event (Budak et al., 2021).

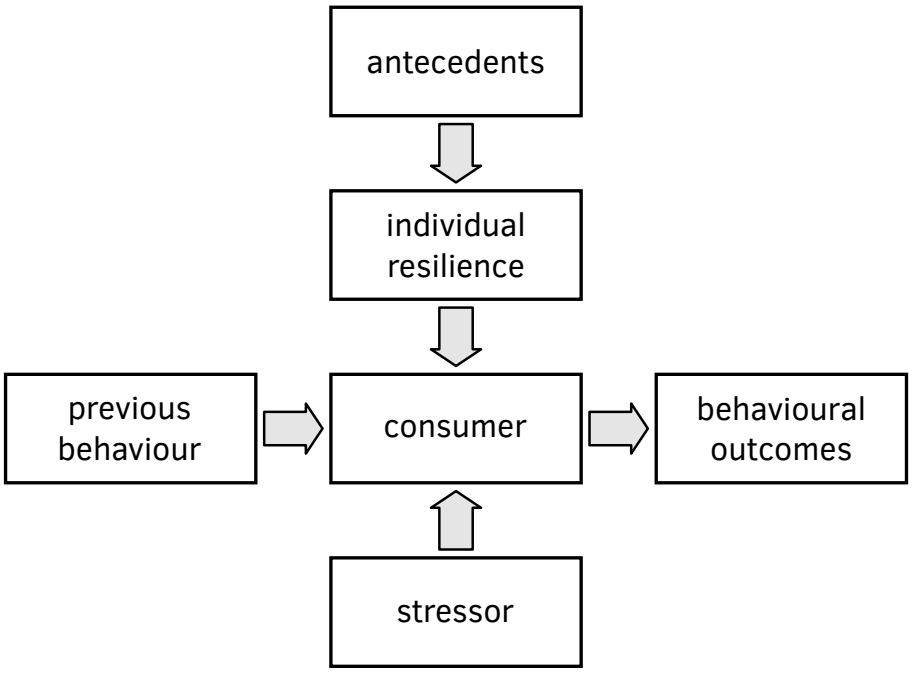


Figure 1: Consumer resilience to privacy violation online [a]

[a]Budak et al. (2021)

## 2.4 Privacy Responsibility – Consumer vs. Service Provider

Rather than placing the responsibility on a single party or stakeholder, Shillair et al. (2015) argue that the responsibility to protect user information online should be shared between users and service providers. Users should rather be encouraged to be more proactive about understanding how their data is used online, as they are currently settling for invasive or exploitative privacy practices at the expense of staying connected (Lipman, 2016). However, even though it seems users are at a disadvantage, Shillair et al. (2015) argue that users have the power to change a company's behaviour based on their reactions to new updates or the development of products that are put out into the market. Proof of this can be seen in WhatsApp's decision to extend its initial deadline for users to accept its January 2021 policy changes based on the criticism it received from the public (Wijoyo et al., 2021). This can be highlighted further by assessing an incident involving Instagram in 2012 (Lipman, 2016). When Instagram announced it was going to change its terms of service and allow users' photos to be sold on or via the platform, the issue gained widespread attention and media coverage. As a result of the public's reaction to the proposed changes, Instagram had to revise its new terms. Thus, there is some evidence to suggest that users do have some degree of influence over how companies handle their data on their behalf.

## 2.5 Privacy Responsibility – Service Provider vs. Government

While service providers are expected to take on the bulk of the responsibility with regard to online privacy, it seems that governments have more freedom to monitor social media data that is available to the public without being subjected to the same degree of regulation as service providers (Baruh et al., 2017). There is still a general expectation that businesses will be held accountable for non-compliance to privacy breaches. Meanwhile, when governments are found to have been abusing surveillance and privacy rights, this tends to be dismissed in favour of them maintaining national security online (Baloyi & Kotze, 2017). Some of the reasons governments would monitor their citizens include analysing social media data for the purposes of fighting crime or terrorism. However, as more people spend more time online and on social media platforms, Di Minin et al. (2021) argue that governments should also be subjected to the same regulations that are imposed on service providers. In summary, the responsibility of ensuring user privacy online should not be the responsibility of a solitary party. Instead, responsibility should be shared between all parties involved, namely the users, the service provider (companies) and governments (where applicable) (Di Minin et al., 2021).

A good example is Europe's enforcement of the GDPR in response to WhatsApp's January 2021 policy changes. The European Union (EU) regulates its citizens' data with strict guidelines set out in its GDPR (MyBroadband Staff Writer, 2021). Because of this, WhatsApp users in select European countries were given the option to opt out of the policy changes, while other users in several developing countries with similar protection policies and regulations were not given the same luxury (Kennedy & Thornberg, 2017). This inconsistent application of the policy highlights the fragmented nature of data protection laws worldwide and how

they are dictated by capital. Therefore, when examining the ideas proposed by Di Minin et al. (2021), it seems these cannot be applied universally. While some governments and similar governing bodies have the means to enact sufficient laws to protect their citizens, others still struggle to implement timely and effective laws to regulate the collection, processing and storage of citizens' data by powerful and omnipresent multinational companies.

## 2.6 International Surveillance Capitalism

Local companies are easier to regulate than multinational ones. Yet despite having some of the best protection policies in the world, policymakers in developing countries are restricted by the fact that several companies that are pivotal to a society's functioning in this digital era are international companies that are bound to their own rules. The most common social media applications used around the world are owned and controlled by a handful of American companies (Kwet, 2020). Furthermore, American companies also own and control some of the most important technological infrastructure required to use these platforms. Services like Netflix are beginning to dominate local television markets globally, while Google and Facebook dominate global advertising and distribution networks. This implies that a significant portion of the user data generated locally belongs to foreign countries.

Zuboff (2019) describes this phenomenon as surveillance capitalism, which is defined as an economic system that focuses on making a profit by collecting and processing personal data. More organisations are becoming dependent on user information for their analytics. User data on social media has thus become capitalised, with social media companies constantly looking to develop new ways of collecting more information from their users. Some of these new methods include competitions, reward programmes and loyalty cards (Kwet, 2020). WhatsApp and Facebook are based in the US, which means American laws are likely to be applied to the data collected from users in other countries. While some countries do have regulations to prevent their citizen's data from being stored outside of their borders, for the most part, the data centres and cloud facilities used to store social media data are based in the US.

This section highlighted that the issue of privacy is important and is becoming more prevalent in the era of social media and how the responsibility of enhancing and ensuring the public's privacy online is still a topic of discussion. There is the view that the responsibility should lie with the individual, while there are the opposing views that it should lie with the private sector or on governments and privacy regulators. Lastly, there is the view that the responsibility should be shared between the stakeholders involved. To get a full sense of how the issue of privacy unfolds, one needs to study all three stakeholders to understand how each of them looks at, understands and responds to the issues of privacy and their roles in this space. This study will target one stakeholder, namely the consumer, where the following sections will explore how WhatsApp users in South Africa view themselves as social media users in terms of online privacy.

https://doi.org/10.18489/sacj.v35i2.17443

## 3 RESEARCH DESIGN

The data for this study was collected through semi-structured interviews. The method used to identify the sample population was the cluster sampling method, where a group of people (adult WhatsApp users) based in a specific geographical location (South Africa) were targeted and approached in their capacity as individuals and asked to participate. Interviews were conducted until a point where the analysis of additional interviews generated little to no new codes or categories (Wolff et al., 2018, Ch.10). Table 1 lists respondents for this study according to age group and professional background.

Table 1: Sample Population Description

| No | Reference | Age Group | Professional Background |
|---|---|---|---|
| 1 | User 1 | 20–30 | Finance |
| 2 | User 2 | 20–30 | Student – Technology |
| 3 | User 3 | 20–30 | Student–Technology |
| 4 | User 4 | 20–30 | Student–Engineering |
| 5 | User 5 | 20–30 | Student–Technology |
| 6 | User 6 | 40–50 | Telecommunications |
| 7 | User 7 | 40–50 | Legal |
| 8 | User 8 | 50–60 | Fin-Tech (Finance and Technology) |
| 9 | User 9 | 30–40 | Digital Marketing |
| 10 | User 10 | 30–40 | Public Health |
| 11 | User 11 | 30–40 | Legal and Insurance |
| 12 | User 12 | 50–60 | Technology |
| 13 | User 13 | 40–50 | Retail and Technology |
| 14 | User 14 | 60+ | Retired (worked in Education) |

The data was analysed abductively using thematic analysis. This means researchers used concepts from some of the theories and frameworks from literature, such as Budak et al. (2021), Schreiner and Hess (2015) and Acquisti and Gross (2006), as a source of inspiration in identifying and interpreting the data to generate codes, categories, and themes (Kennedy & Thornberg, 2017). The emerging themes were used to group, make sense of, and describe respondents' influences and reactions to the policy changes. Figure 2 displays the evolution of the data analysis process.

## 4 RESULTS

The findings show that the most significant influences that affected how users reacted to the policy changes came from what they knew (awareness) and thought about the policy (perceptions). In addition to individual perceptions and general behavioural patterns regarding

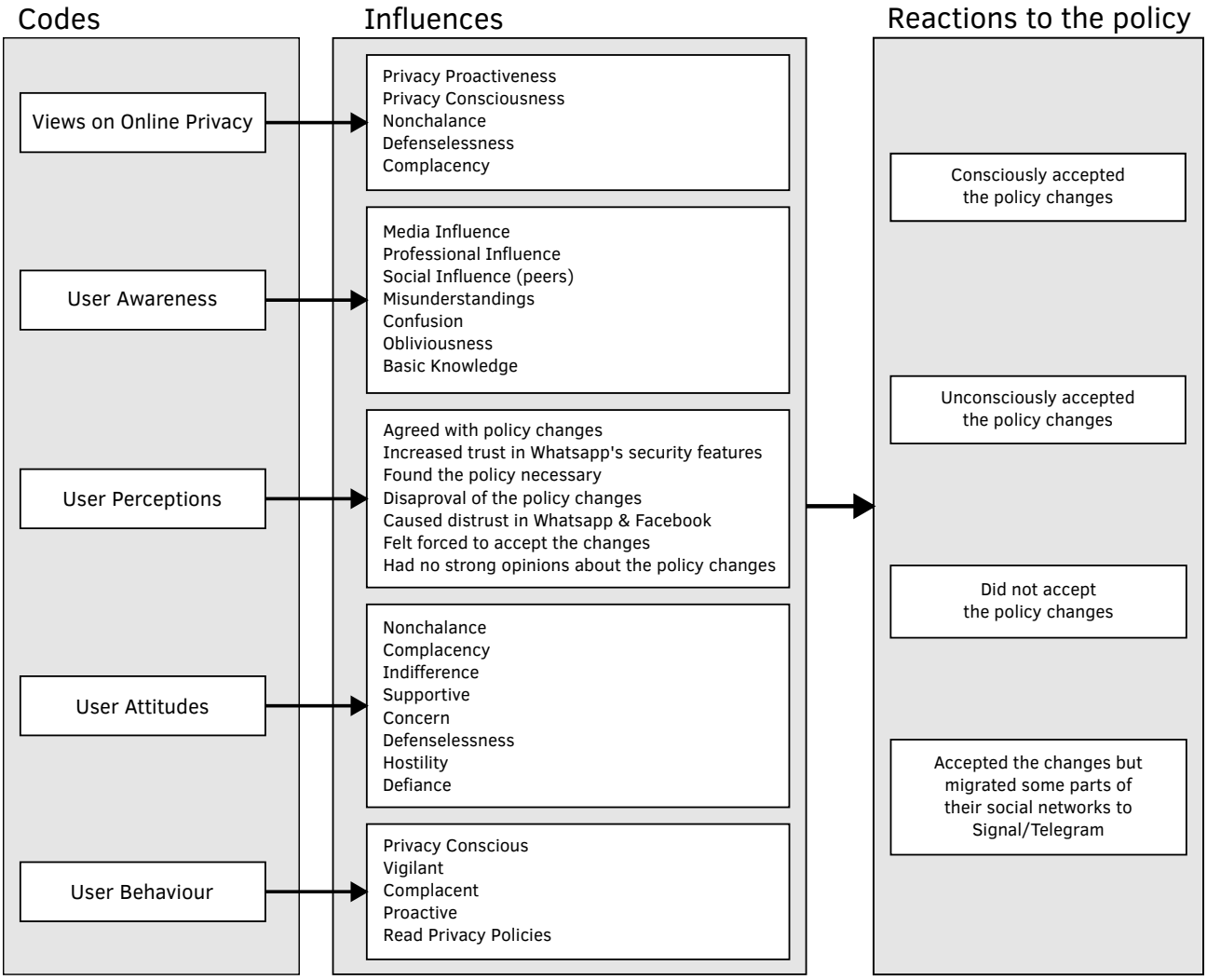


Figure 2: A data structure depicting the evolution of the thematic analysis from codes to key themes

online privacy, individualistic factors also influenced users' reactions to the policy changes. An example of this is seen with User 12, who is one of the older participants, and described themselves as a

*"baby boomer (who) grew up with more face-to-face interactions",*

or User 13, who understands the value of

*"building a portfolio (of) consumer data"*

due to their professional background in digital marketing. Both participants, however, disapproved of the policy changes, despite the contrasting individual factors described previously.

https://doi.org/10.18489/sacj.v35i2.17443

It can therefore be assumed that the unique combination of a user's knowledge about, perceptions of, and attitudes towards the policy, coupled with their general behaviour on social media, influenced their reactions to the policy changes to some extent. Further individual characteristics that influenced users' reactions are discussed below.

## 4.1 What did South African users know about the policy?

When examining how much users knew about the policy, it was found that users had some knowledge of the policy but not extensive knowledge of what it entailed or how it would impact them. In other words, users gave a spectrum of answers to describe the extent to which they knew about the policy, which ranged from obliviousness to basic knowledge to partial knowledge about the changes.

Some users were more aware of the policy because of their professional backgrounds. For example, people who had a legal or technological background appeared to understand the policy relatively more compared to users who did not

> *"… really know the details",* [User 10]

or who were only

> *"aware that there was a policy that was introduced"* [User 1]

from the media. None of the users fully understood what the policy entailed or how it would impact them and their usage of WhatsApp. None of the users had also taken the time to read the policy. What was also discovered from the results is that users are no longer as conscious of the policy compared to when it was introduced. As put by one of the users:

> *"I don't think about it on my day-to-day anymore. I'm only thinking about it now that you've mentioned it to me."* [User 4]

## 4.2 What did South African users think about the policy?

Perceptions about the policy changes differed, with users giving a range of responses. Some users objected to the policy changes and were not supportive of them, some users did not have any strong opinions about the changes, and some users were supportive of the policy changes.

In general, there were fewer users, such as those with a legal background, who supported the changes, with one user stating:

> *"I work in the legal department, and we actually have to know about these policies. The policy is a good thing because some companies will just go ahead and share your information with third parties without your consent. But at least with this policy, there is a preventative measure in place that provides safety for users and a means to take legal action."* [User 7]

https://doi.org/10.18489/sacj.v35i2.17443

Some users expressed that they were in favour of accepting the policy changes because their levels of trust with WhatsApp were higher compared to other instant messengers and social media platforms. In summary, users favouring the policy found it a

*"necessary thing to have."* [User 7]

When the policy was introduced, WhatsApp received widespread criticism from the public. However, users' perceptions of the policy changes were generally expressed as indifference, with users stating WhatsApp's accessibility and lack of alternatives for central communication as their main reasons for staying with the service. It was also deemed too much of an effort to restructure one's social networks by moving parts of it to Telegram and/or Signal. One user's response highlights this:

*"If I don't use WhatsApp, what am I going to use because it's going to be difficult to move everyone I know over to Telegram."* [User 2]

These feelings of nonchalance, complacency, indifference and even defencelessness towards the policy were still maintained even after users were made aware of how some users based in select European countries were exempted from accepting the policy changes. As seen with [User 8], even when given a choice, WhatsApp users based in South Africa were likely to have accepted the policy, but

*"it would have been nicer if [they] had [been given] the choice"*

to opt-out.

Lastly, this part of the results will look at the responses from the users who had not accepted the policy changes when they were interviewed. These users felt

*"forced to agree to something [they were] not comfortable with"* [User 12]

and decided that the cost of trading their privacy was a bigger loss. These users did not view WhatsApp as crucial to their networks in comparison to the other users in the sample, with one user stating,

*"I'm not happy about it … I can live without it [WhatsApp]."* [User 11]

## 4.3 How did South African users react to the policy changes?

In general, users accepted the policy, but there is evidence to suggest that users did so out of necessity and not choice, with one user stating:

*"you have to accept it for you to continue having the platform."* [User 10]

https://doi.org/10.18489/sacj.v35i2.17443

A few users consciously chose to accept the policy after taking the time to research its implications briefly. However, a significant portion of the sample that had accepted the policy had done so unconsciously. Not one user had taken the time to read the policy in-depth before accepting it, despite users from the sample identifying themselves as privacy-conscious individuals who are proactive about protecting their data.

All users, even the few who had not accepted the policy changes at the time, verified that they were still using WhatsApp due to how central it is to their communication with their social networks. Initially, users switched to another service when the policy was introduced, with the most popular choice for this sample being Telegram. A few other users opted for Signal. However, all users who switched stated that they were attracted back to WhatsApp due to its end-to-end encryption feature that they felt was lacking on other platforms.

## 5 DISCUSSION

As highlighted in the results, several factors influence how users respond to online privacy breaches or manage themselves online. Some factors can be generic, but the most significant influences come from a user's unique point of reference.

### 5.1 Online Privacy and User Behaviour

One theme that emerged from the data was that of online privacy. Users described themselves as privacy-conscious individuals who are vigilant when using social media. However, no users had taken the time to understand the policy in-depth when it was introduced. Furthermore, despite the spectrum of opinions regarding the policy changes, all users who were interviewed were still using WhatsApp at the time since it was the most convenient option for them.

This behavioural pattern matches the observations made by Schreiner and Hess (2015), where it was found that users would continue their use of an online service they are generally dissatisfied with due to the social opportunity costs and networking factors involved. Acquisti and Gross (2006) emphasise this point further. The authors argue that users' actions rarely affect their concerns in the event of a privacy breach. An example of this was observed with the Facebook and Cambridge Analytical data breach. Though there were several calls from privacy regulatory bodies and the media for users to close their Facebook accounts, it was found that users did not even take the time to alter their privacy settings, let alone discontinue their use of the app (Hinds et al., 2020). Similarly, the WhatsApp users participating in this study continued to use the app, despite their concerns.

This behaviour contrasts what would generally be expected from a privacy-conscious individual. Privacy-conscious individuals or 'privacy actives' are characterised by high standards and expectations of privacy policies. If privacy actives were dissatisfied with a service, they would not hesitate to discontinue using it (Redman & Waitman, 2020). The users who participated in this study identified themselves as privacy-conscious individuals who are attentive to how their data is used and shared online. However, their behaviour, as highlighted by the

evidence in the results and by multiple studies mentioned in the background, did not match their beliefs.

## 5.2 Macro and Micro-Economic Influences

The results from Section 4.3 also highlighted how a combination of influences unique to an individual influenced their reactions to the policy changes. This is supported by Budak et al. (2021), who state that when affected by an online privacy breach or a stressor, users' reactions are likely to be influenced by a combination of factors that would differ with each person. As observed with this group of users, the combination of what they knew and thought about the policy influenced their reactions. Using terminology provided by Budak et al. (2021), these influences would be described as macroeconomic factors. However, there were other influences, which were not as impactful as the previous two, that also influenced a user's reactions to the policy to some extent. These would be described as the micro-economic factors, which include a user's age, professional background, and general attitudes towards social media, WhatsApp and online privacy. Therefore, when putting the model developed by the authors in the context of this topic, the framework illustrated in Figure 3 would apply.

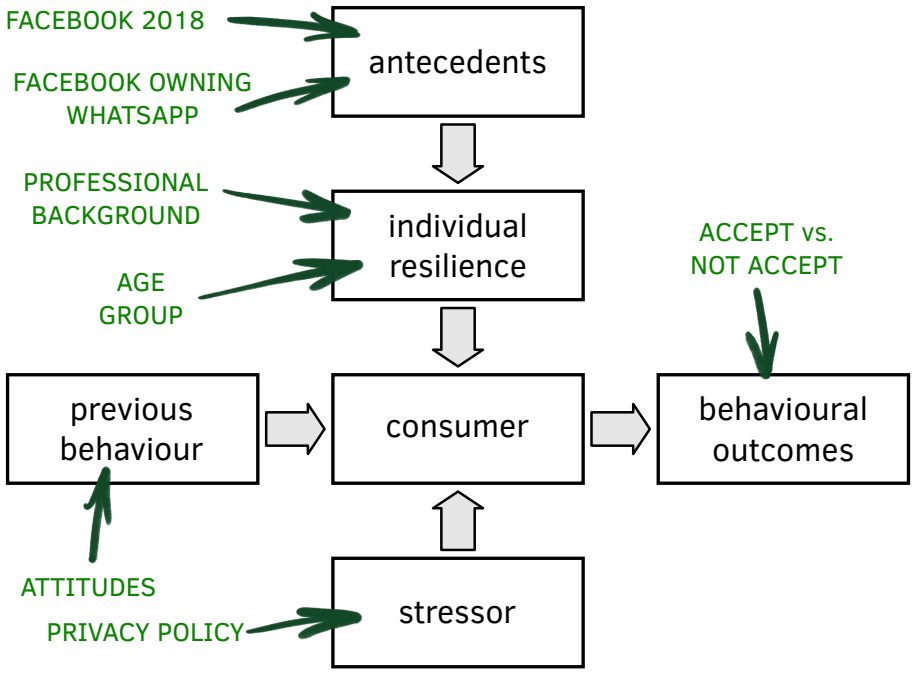


Figure 3: Updated research framework of consumer resilience to privacy violation online

The consumer becomes the user and the stressor becomes WhatsApp's January 2021 privacy policy. The antecedents that influenced the behavioural outcomes for this group of users

were WhatsApp's relationship with Facebook, with users linking the 2021 incident with the 2018 Facebook-Cambridge Analytica publicised event. Users who had strong, negative perceptions of this preceding event, and Facebook, disapproved of the policy changes and refused to accept them at the time of the interview. Further micro-economic factors such as an individual's professional background or age were also observed to have influenced a user's reactions to the policy changes. An example of this can be seen with users who have a background in the legal field. These users also had negative perceptions of Facebook but were supportive of the policy due to their understanding of how and why privacy legislation is designed and implemented. Therefore, as described in the results, the updated diagram in Figure 3 can be used along with the data structure presented in the results to gain further insight into this social phenomenon.

## 5.3 User Attitudes Towards Online Privacy

Users generally seemed indifferent, nonchalant, and complacent when asked about their opinions on the policy changes. These feelings and attitudes remained even when they were informed about how the policy was distributed unequally. This issue becomes more prevalent in developing countries like South Africa, where the most accessible social networking platforms are developed and owned by large multinational corporations. The issue observed is that the regulatory bodies in said developing countries struggle to enforce their legislature and regulations on these corporations to protect their citizens. This leaves users in these economies vulnerable to potential exploitation from service providers. As a consequence, noting that the options they can use to protect themselves are limited, coupled with the fact that their regulatory bodies do not have the requisite influence to deter these corporations, social media users in developing counties begin to develop attitudes of defencelessness, complacency, and indifference in events like this despite being dissatisfied with the situation.

Because of the pervasiveness of social media, the issue of responsibility in enhancing privacy for users online is still a topic of discussion. As seen through the Cisco study (Redman & Waitman, 2020), users would like to be more proactive about ensuring their privacy online but feel that their autonomy is limited. Hence, users place the expectation of ensuring their privacy on the private sector and service providers like WhatsApp. Where the private sector fails, the expectation is then placed on governments and policy regulatory bodies to intervene on behalf of the consumer (Ahad & Lim, 2014).

# 6 CONCLUSION AND RECOMMENDATIONS

This study explored how consumers view and perceive their role in ensuring online privacy. Based on the findings and discussion, we see that users have little influence in safeguarding their online privacy. This is because they are often put in a position where they must choose convenience at the expense of their privacy to maintain using their social networks, despite

this going against their best interests. An example of this can be seen in how WhatsApp users based in South Africa responded to the January 2021 policy changes.

Despite the overall criticism WhatsApp received when the policy was introduced, users generally had neutral perceptions about the policy and accepted the terms without much resistance or conscious effort. WhatsApp was already a central point of communication for people in South Africa before the pandemic, as work, school and personal networks were all managed on the platform. Users thus accepted the policy out of necessity because the opportunity costs they would have incurred to restructure their social networks seemed too significant. The disparity in regulatory enforcement between countries has also left users to act on their own, as most developing countries do not have privacy laws that are strong enough to protect their users.

It is recommended that researchers use this study as grounds for further large-scale research to observe and understand how the other two stakeholders (corporations and governing bodies) perceive and understand their roles in the digital space. This study has provided some insight into why users tend to behave the way they do online. However, further research is required to develop an in-depth understanding of how privacy issues unfold between all three stakeholders.

## References

Abbas Naqvi, M. H., Jiang, Y., Miao, M., & Naqvi, M. H. (2020). The effect of social influence, trust, and entertainment value on social media use: Evidence from Pakistan (Y. J. Wu, Ed.). *Cogent Business & Management*, *7*(1), 1723825. https://doi.org/10.1080/23311975.2020.1723825

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Lecture notes in Computer Science* (pp. 36–58). Berlin Heidelberg, Springer. https://doi.org/10.1007/11957454_3

Ahad, A. D., & Lim, S. M. A. (2014). Convenience or Nuisance?: The 'WhatsApp' Dilemma. *Procedia – Social and Behavioral Sciences*, *155*, 189–196. https://doi.org/10.1016/j.sbspro.2014.10.278

Baloyi, N., & Kotze, P. (2017). Are organisations in South Africa ready to comply with personal data protection or privacy legislation and regulations? *2017 IST-Africa Week Conference (IST-Africa)*, 1–11. https://doi.org/10.23919/istafrica.2017.8102340

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review: Privacy concerns meta-analysis. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Beigi, G. (2018). Social media and user privacy. *2018 International Conference on Social Computing, Behavioral-Cultural Modeling, & Prediction and Behavior Representation in Modeling and Simulation*, *abs/1806.09786*. http://arxiv.org/abs/1806.09786

Bhattacharjee, A., & Dana, J. (2017). People think corporations can't do good and make money. Can companies prove them wrong? *Harvard Business Review, November 28, 2017*. https://www.brandreality.se/wp4/wp-content/uploads/2018/11/HBR.pdf

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, *48*(7), 953–977. https://doi.org/10.1177/0093650218800915

Bonanno, E. R. (2014). The social media paradox: An examination of the illusion versus the reality of social media. *Sociological Imagination: Western's Undergraduate Sociology Student Journal*, *3*(1), 1–4. https://ojs.lib.uwo.ca/index.php/si/article/download/5271/4416/

Budak, J., Rajh, E., Slijepčević, S., & Škrinjarić, B. (2021). Conceptual research framework of consumer resilience to privacy violation online. *Sustainability*, *13*(3), 1238. https://doi.org/10.3390/su13031238

Cadwalladr, C. (2018). Facebook suspends data firm hired by Vote Leave over alleged Cambridge Analytica ties [7 April 2018]. *The Guardian*. https://www.theguardian.com/us-news/2018/apr/06/facebook-suspends-aggregate-iq-cambridge-analytica-vote-leave-brexit

Church, K., & de Oliveira, R. (2013). What's up with WhatsApp?: Comparing mobile instant messaging behaviors with traditional SMS. *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, 352–361. https://doi.org/10.1145/2493190.2493225

Compañó, R., & Lusoli, W. (2010). The policy maker's anguish: Regulating personal data behaviour between paradoxes and dilemmas. In *Economics of information security and privacy* (pp. 169–185). Springer US. https://doi.org/10.1007/978-1-4419-6967-5

Di Minin, E., Fink, C., Hausmann, A., Kremer, J., & Kulkarni, R. (2021). How to address data privacy concerns when using social media data in conservation science. *Conservation Biology*, *35*(2), 437–446. https://doi.org/10.1111/cobi.13708

Duggan, M., Ellison, N. B., Lampe, C., Lenhart, A., & Madden, M. (2015). Pew research center: Social media update 2014. https://www.pewresearch.org/internet/2015/01/09/social-media-update-2014/

Fiesler, C., & Hallinan, B. (2018). "We are the product": Public reactions to online data sharing and privacy controversies in the media. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3173574.3173627

Gibbs, J. L., Ellison, N. B., & Lai, C. (2010). First comes love, then comes Google: An investigation of uncertainty reduction strategies and self-disclosure in online dating. *Communication Research*, *38*(1), 70–100. https://doi.org/10.1177/0093650210377091

Goldstuck, A. (2012). Internet matters: The quiet engine of the South African economy. *World Wide Worx*, *236*. https://hsf.org.za/publications/focus/focus-66/AGoldstuck.pdf

Hashimzade, N., Myles, G. D., Page, F., & Rablen, M. D. (2014). Social networks and occupational choice: The endogenous formation of attitudes and beliefs about tax compliance.

*Journal of Economic Psychology*, *40*, 134–146. https://doi.org/10.1016/j.joep.2012.09.002

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, *143*, 102498. https://doi.org/10.1016/j.ijhcs.2020.102498

Kennedy, B. L., & Thornberg, R. (2017). Deduction, induction, and abduction. In U. Flick (Ed.), *The SAGE handbook of qualitative data collection*. SAGE Publications Ltd. https://methods.sagepub.com/book/the-sage-handbook-of-qualitative-data-collection

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: why we disclose. *Journal of Information Technology*, *25*(2), 109–125. https://doi.org/10.1057/jit.2010.6

Kwet, M. (2020). Surveillance in South Africa: From skin branding to digital colonialism. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3677168

Lipman, R. (2016). Online privacy and the invisible market for our data. *Network Security*, *2004*, 18–19. https://doi.org/10.1016/S1353-4858(04)00120-5

Montag, C., Błaszkiewicz, K., Sariyska, R., Lachmann, B., Andone, I., Trendafilov, B., Eibes, M., & Markowetz, A. (2015). Smartphone usage in the 21st century: Who is active on WhatsApp? *BMC Research Notes*, *8*(1). https://doi.org/10.1186/s13104-015-1280-z

Mugadza, K., & Mwalemba, G. (2022). Online platform privacy policies: South frican Whatsapp users' perceptions and reactions to the January 2021 changes. In A. Gerber (Ed.), *Proceedings of 43rd conference of the south african institute of computer scientists and information technologists* (pp. 214–230, Vol. 85). EasyChair. https://doi.org/10.29007/m9d5

MyBroadband Staff Writer. (2021). WhatsApp privacy concerns in South Africa explained. https://mybroadband.co.za/news/security/384886-whatsapp-privacy-concerns-in-south-africa-explained.html

Nobre, G. P., Ferreira, C. H., & Almeida, J. M. (2022). A hierarchical network-oriented analysis of user participation in misinformation spread on WhatsApp. *Information Processing & Management*, *59*(1), 102757. https://doi.org/10.1016/j.ipm.2021.102757

Parez, S. (2020). Whatsapp has seen a 40% increase in usage due to COVID-19 pandemic [TechCrunch]. https://techcrunch.com/2020/03/26/report-whatsapp-has-seen-a-40-increase-in-usage-due-to-covid-19-pandemic/

Perrin, A. (2015). Social media usage: 2005-2015. https://www.pewresearch.org/internet/2015/10/08/social-networking-usage-2005-2015/

Rajpurohit, G. S., & Yadav, R. K. (2021). A socio-legal analysis of Whatsapp privacy policy 2021 in India: A contemporary study. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3850579

Redman, T. C., & Waitman, R. M. (2020). Do you care about privacy as much as your customers do? https://hbr.org/2020/01/do-you-care-about-privacy-as-much-as-your-customers-do

Schreiner, M., & Hess, T. (2015). Examining the role of privacy in virtual migration: The case of WhatsApp and Threema. *AMCIS 2015 Proceedings*. https://aisel.aisnet.org/amcis2015/ISSecurity/GeneralPresentations/33

Shambare, R. (2014). The adoption of Whatsapp: Breaking the vicious cycle of technological poverty in South Africa. *Journal of Economics and Behavioral Studies*, *6*(7), 542–550. https://doi.org/10.22610/jebs.v6i7.515

Shillair, R., Cotten, S. R., Tsai, H. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing internet users to protect themselves. *Computers in Human Behavior*, *48*, 199–207. https://doi.org/10.1016/j.chb.2015.01.046

Smit, E. G., Van Noort, G., & Voorveld, H. A. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, *32*, 15–22. https://doi.org/10.1016/j.chb.2013.11.008

Smyth, B. (2014). *Forget Me Do: Empowering user privacy on social network sites* (tech. rep. No. 2014/10). Forget Me Do Limited. https://publications.bensmyth.com/2014-privacy-on-social-network-sites/

Stieger, S., Burger, C., Bohn, M., & Voracek, M. (2013). Who commits virtual identity suicide? Differences in privacy concerns, internet addiction, and personality between Facebook users and quitters. *Cyberpsychology, Behavior, and Social Networking*, *16*(9), 629–634. https://doi.org/10.1089/cyber.2012.0323

Wijoyo, H., Limakrisna, N., & Suryanti, S. (2021). The effect of renewal privacy policy Whatsapp to customer behavior. *Insight Management Journal*, *1*(2), 26–31. http://repository.upi-yai.ac.id/3136/

Wolff, B., Mahoney, F., Lohiniva, A. L., & Corkum, M. (2018). Collecting and analyzing qualitative data. In S. A. Rasmussen & R. A. Goodman (Eds.), *The CDC field epidemiology manual*. https://www.cdc.gov/eis/field-epi-manual/chapters/Qualitative-Data.html

Zuboff, S. (2019). Surveillance capitalism and the challenge of collective action. *New Labor Forum*, *28*(1), 10–29. https://doi.org/10.1177/1095796018819461