EPiC Series in Computing

Volume 85, 2022, Pages 214–230

Proceedings of 43rd Conference of the South African Institute of Computer Scientists and Information Technologists

EPiC Computing

Online Platform Privacy Policies: South African WhatsApp Users' Perceptions and Reactions to the January 2021 Changes

Kimberley Mugadza[1,2*] and Gwamaka Mwalemba[1†]

[1] EasyChair

[2] University of Cape Town, Cape Town, South Africa.

kimberley.mugadza@alumni.uct.ac.za, gt.mwalemba@uct.ac.za

Abstract

On the 4th of January 2021, WhatsApp proposed a policy update that required its users to consent to have some of their data on the application linked to Facebook to boost the commercialisation of their users' data for their insights. The move received widespread attention and criticism from some users, media, regulators, and organisations that have an interest in user data protection. The pervasiveness of WhatsApp meant that close to 2 billion users around the world were likely to be impacted by the policy. The event also caused some further debate about the ethical standards of individuals' privacy and data security online. This qualitative interpretive case study aims to explore what WhatsApp users based in South Africa knew about the policy, how they perceived it, and how their perceptions influenced their reactions to the policy and WhatsApp usage in general. The results suggest that users who were studied accepted the policy out of necessity, not choice, citing WhatsApp's omnipresence and lack of similarly ubiquitous alternatives as their main reasons for staying with the service.

1 Introduction

WhatsApp introduced a new privacy policy on the 4th of January 2021 which users would have seen 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 their data on the app linked to Facebook by no later than the 15th of May 2021 (Limakrisna, Suryanti & Wijoyo, 2021).

[*] Masterminded EasyChair and created the first stable version of this document

[†] Created the first draft of this document

This date was extended from the initial deadline (which was set to 8 February 2021) because of the general confusion over the new policy (Somari, 2021).

The main concern was caused by a clause which describes how the policy would focus more on users' interactions with business accounts. In summary, the new policy would allow registered business accounts to *"...provide third-party service providers with access to their communications to send, store, read, manage, or process them for the business"*, (Zuboff, 2019). This means that if users communicate with businesses on WhatsApp, businesses could be sharing their data with third-party service providers without their knowledge (Limakrisna, Suryanti & Wijoyo, 2021).

Because of this, WhatsApp received criticism from its users with users beginning to consider closing their accounts and migrating to similar messengers like Telegram and Signal (Limakrisna, Suryanti & Wijoyo, 2021). This decision, however, was not simple because WhatsApp has become a central point of communication for many users with many activities, like online learning during the covid-19 pandemic, being carried out on the platform.

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 lockdown with more users using WhatsApp to stay connected with family members, friends, and colleagues (Perez, 2020). WhatsApp is no longer a simple instant messenger that can be used for socialising; 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 (Perez, 2020). WhatsApp was already a central platform of communication for South Africans before the pandemic. The current circumstances brought by the COVID-19 pandemic have only heightened WhatsApp's relevance in South African society as more aspects of people's lives migrated online. Thus, because of their dependency on WhatsApp services, users in South Africa received WhatsApp's proposed privacy policy with resistance (Fiesler & Hallinan, 2018).

The event regarding WhatsApp's January 2021 privacy policy has also been linked to a similar online privacy breach that happened in March 2018 with Facebook and Cambridge-Analytica. It was revealed that Cambridge Analytica, a data collections company, had been collecting data from approximately 87 million Facebook users' profiles. This data was used to customise the advertisements users would see while using Facebook. It was alleged that these tailored advertisements were made to influence Americans' voting preferences in the 2016 US presidential election (Hinds, Joinson & WIlliams, 2020). This incident became one of the most publicised data breaches of the year because several 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.

In the case of WhatsApp, the privacy policy affected all of WhatsApp's 2 billion users around the world. When the company was bought by Facebook in 2014, users were reassured that there were no plans to share their data with third parties. However, the supposed change in stance shown by the introduction of the policy, Facebook-Cambridge Analytica and similar privacy policy events have thus created a lack of trust from users and a perception that corporations are prioritising profit over user wellbeing (Bhattacharjee & Dana, 2017). Incidents like the ones described previously have also started causing 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, Joinson & WIlliams, 2020).

1.1 Research Objectives, Questions and Scope

This study is a qualitative interpretive study that looks to understand the reasons behind users' reactions to the policy. This will be achieved by fulfilling the following objectives and answering the following research questions:

Main Objective: To explore how WhatsApp users based in South Africa have reacted to the changes in WhatsApp's January 2021 privacy policy.

Sub-Objective 1: To explore what WhatsApp users in South Africa know about the terms set out in the privacy policy.

Sub-Objective 2: To explore how WhatsApp users in South Africa perceive the policy changes.

Sub-Objective 3: To explore how WhatsApp users in South Africa have reacted to the policy changes.

Main Research Question: How have WhatsApp users in South Africa reacted to the changes in WhatsApp's January 2021 privacy policy?

Sub-Question 1: What do WhatsApp users in South Africa know about the changes in WhatsApp's January 20201 privacy policy?

Sub-Question 2: What do WhatsApp users in South Africa think about the changes in WhatsApp's January 2021 privacy policy?

Sub-Question 3: How have WhatsApp users in South Africa reacted to the recent changes in WhatsApp's January 2021 privacy policy?

WhatsApp also received criticism about its policy because of its unequal distribution with users in some European countries being exempt accepting the policy changes. 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 discontinued. This limited the autonomy users would have had regarding their decision over this policy. A few studies about this policy have been found from other countries. An example of such a study is authored by Limakrisna, Suryanti & Wijoyo, (2021), which studies the perceptions users in Indonesia had to this policy when it was proposed. Another example of such a study includes a socio-legal analysis of the new policy authored by Rajpurohit and Yadav (2021) in India. Currently, no research or studies looking at this phenomenon from a South African perspective has been found. This study, therefore, aims to explore what perceptions and reactions WhatsApp users in South Africa had to the January 2021 privacy policy where the results and themes found from the data will be used to describe the social phenomenon in a local context.

1.2 Overview

This empirical report will begin with a literature review which will explore the themes and concepts of online privacy and social media. Next, the research methodologies which outline and justify the methods used to carry out this study will be discussed. These methods include a description of the data collections process, the research instruments that were used, a description of the sample population observed for this study, the analysis methods used, and the ethical standards adopted. The key insights found from the data will then be presented, analysed, and linked to the literature in the Findings and Discussion. The study will be concluded by showing how the Findings and Analysis fulfilled the research objectives and questions.

2 Literature Review

In recent years, there have been several privacy-related debates and events that 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). Because of these recurring privacy-related events, technology designers and policymakers are now being held more accountable by their users. Consequently, these policymakers and designers are now being faced with the challenge of balancing out their users' unpredictable privacy habits with regulations and guidelines regarding the personal data that is collected from users (Compañó & Lusoli, 2010). This literature review will explore and analyse the current literature available on the topics of online privacy, social media usage and international surveillance capitalism. The review will then be concluded with a summary highlighting the main concepts found in the literature and linking them to the topic.

2.1 Social Media and Online Privacy

The shift from traditional mass media (such as receiving news from the news or newspapers) to personal media for mass self-communication (such as receiving news from social networking sites (SNS) and micro-blogs) is becoming commercially engrained in daily life (Pierson, 2014). The common belief within modern society is that users have complete autonomy over their socio-technical innovation. There is, however, a paradox that is observed which is noted by Smyth (2014). On one hand, the use of social media can be empowering for users because SNS seemingly offer their users total creative control over the representations of their identities online (Bonanno, 2014). Online users, however, do 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 to share their data with either the SNS service provider or another third party in some form. This would have implications on overall user privacy, autonomy, and empowerment (Beigi, 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 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 been known as "privacy actives". 90% of the privacy actives identified from the sample population believed that the way their data is used reflects how they will be treated as users. Based on these results, it was concluded that privacy actives are, therefore, unlikely to interact with a social media platform, application and (or) business where they do not trust how their data is going to be used (Redman & Waitman, 2020).

When asked if 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 what data will be used for which purpose (Redman & Waitman, 2020). The survey results also revealed that privacy actives are the most likely to read privacy policies – 83% actively do. However, the consensus within the sample population was that the language used in these policies can be unclear to the average person. Respondents also stated that having a detailed privacy policy or "Terms of Use" page is useful but taking the time to sort through it can be impractical because of 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, therefore, implies that users expect more of the responsibility about their data to be that of service providers like WhatsApp (Alhabash et. al, 2015).

Contrary to the study by Redman and Waitman (Redman & Waitman, 2020), prior research by Acquisiti and Gross (Acquisiti & Gross, 2006) showed that when forced to choose, users are more likely to choose convenience over their privacy. This behavioural pattern was observed even in users who ranked their privacy concerns quite high in comparison to other societal issues (Hess & Schreiner, 2015). Additionally, users generally view the perceived benefits of using social media services as a sufficient incentive to trade their privacy at the cost of their convenience (Bohn, Burger, Stieger & Voracek, 2013).

A study was conducted in 2015 by Hess and Schreiner (Hess & Schreiner, 2015) which explored whether users would be willing to switch from one service to another over privacy concerns. It was found that dissatisfaction with privacy practices have a stronger effect in influencing users to discontinue their use of a service over the attractiveness of a sound privacy policy (Hess & Schreiner, 2015). However, despite this observation, Hess and Schreiner (Hess & Schreiner, 2015) also observed that it is more common for users to be unwilling to switch services. This is mainly attributed 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 (Acquisiti & Gross, 2006)

There is, however, also some evidence to suggest that users are likely 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).

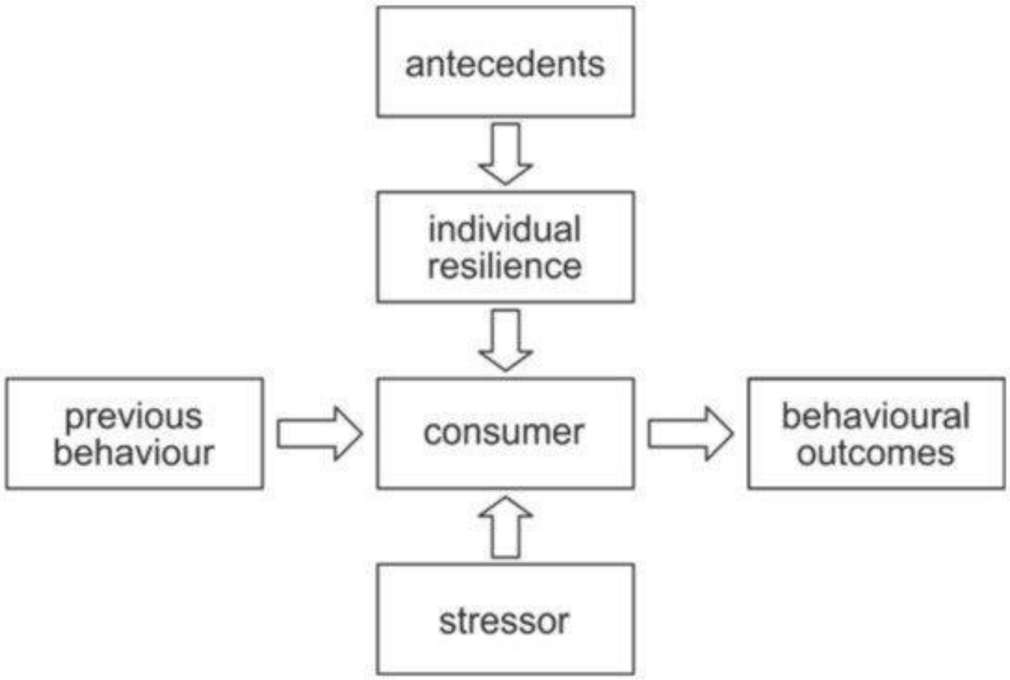

Figure 1. Research framework of consumer resilience to privacy violation online (Budak et.al, 2021)

When a consumer (user) is affected by a stressor like an online privacy breach, the user is likely to respond to this event with resistance. The level of resistance is likely to be influenced by the user's knowledge about and perceptions of a similar event. This is shown in the diagram as the antecedent which influences an individual's level of resistance (Budak et.al, 2021). Users' reactions to an online privacy breach are also influenced by micro and macro-economic factors such as their educational and professional background, their age, their level of income, individual attitudes towards internet usage and their 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).

2.4 Distribution of the Policy – European vs Non-European Countries

One of the issues regarding the privacy policy related to its inconsistent application where European and non-European countries seemed to have received different terms of service for the privacy policy. The reason for this was attributed to the European Union regulating its citizens' data with strict GDPR guidelines (Adams, 2021). However, South Africa's privacy legislation, The Protection of Personal Information (POPI) Act, compares strongly to the GDPR and is stricter than the GDPR in some ways. Hence the same standards that were applied to the exempt European countries should have been applied to any non-European country with similar privacy regulations. The inconsistent application of the policy thus highlights the fragmented nature of data protection laws around the world and how they are dictated by power.

Had WhatsApp been a South African company, it would have been easier to regulate. Yet, despite having one of the best protection policies in the world, South African lawmakers and regulators are constrained by the fact that WhatsApp is a foreign company with a large local and international user base. This phenomenon does not start and end with WhatsApp as most of the widely used social media applications in South Africa are owned and controlled by a handful of international companies (Kwet, 2020). Services like Netflix are beginning to dominate the local television market in the country, while Google and Facebook are dominating the country's advertising and distribution networks. This implies that a significant portion of the user data generated in the country is managed and processed by foreign technology companies. These companies have also grown to become large multinationals with budgets and user bases bigger than that of several countries combined. This leaves multinationals with a window to use their ability to influence users and policies in their favour by using their unlimited capital to expand their wealth, all while exploiting their already well-established and often unsuspecting customer bases.

The phenomenon described previously can be defined as surveillance capitalism which is defined as an economic system that focuses on making a profit by collecting and processing personal data (Zuboff, 2019). Mainstream social media services and similar platforms are free to use as users can sign up and use these services of their own free will without incurring any charges (Gruzd, Hernández-Garcia & Jacobson, 2020). There are, however, other methods that consumers use to pay for their use of these services such as giving consent to having their data shared with companies. Several social media platforms generate an income by displaying tailored advertisements to their consumers – advertisements that can only be personalized accurately with adequate data (Lipman, 2015). Thus, more organisations are becoming dependent on user information for their analytics which has led to the capitalization of user data on social media (Kwet, 2020). This has also resulted in companies constantly trying to develop new ways of collecting more information from their users.

2.5 Summary

Recurring themes and notions about user behaviour in the context of online privacy were found throughout the literature. Though individuals are becoming more proactive about voicing their demands for better management of their data, their actions rarely reflect their concerns. Instead, it seems that the perceived benefits of using social media services provide users with sufficient incentive to trade their online privacy at the cost of convenience. Several examples were found in the literature to substantiate this including the well-publicized Facebook and Cambridge Analytica case. Despite the numerous calls from the public for users to close their Facebook accounts, users simply continued to use Facebook with few making some changes to their privacy settings. There are, however, other factors that influence user behaviour in this context, all of which will differ from user to user. Though convenience could have been a significant factor that influenced this general behaviour, the combination of users' attitudes, preferences and beliefs regarding online privacy also play a role in influencing their behaviour online. Another factor that was not discussed extensively in literature could be external influences from peers and the media. The incidents with WhatsApp and Facebook both received widespread media coverage, with both companies receiving criticism from the public. Findings from the Cisco survey revealed that most users do not read privacy policies or terms and conditions in depth. This creates the impression that users are not fully aware of what they are consenting to or how their data is used by companies. There is therefore a possibility that users' understanding, perceptions and attitudes about online privacy is influenced to some extent by the information received from the media and their peers. These influences will also have an impact on how users manage themselves online, thus emphasizing the relevance of studies that explore, understand and contextualize user habits in these environments.

3 Research Methodology

This study was a cross-sectional, qualitative interpretive study that focused on understanding how users based in South Africa perceived the terms outlined in WhatsApp's January 2021 privacy policy. The study also explored how users' perceptions of the policy influenced their reactions.

An interpretive philosophy was adopted for this study as the aim was to understand these factors from the perspective of the subjects (WhatsApp users in South Africa). To fulfil the objectives of this study, it was crucial to interpret what users were communicating as this became useful in describing the phenomenon in more depth and validity during the data analysis. These interpretations were also used to understand the factors which influenced the behaviours in the social context of this study.

The approach to theory for this research was inductive where the experiences, observations and insights about the population were abstracted to derive a general truth about how users are likely to react in a similar phenomenon (Cohen, Copi & Flage, 2006). Though models that apply to this study were found during research and described in the literature, they were not used to guide the data collections process. Instead of assuming things about the population at the beginning, this study aimed to explore and understand the root influences behind users' reactions, some of which can be linked to relevant theories described in the literature review (Kigo & Varpio, 2020). Therefore, an inductive approach was the most appropriate for this study.

3.1 Data Collection and Analysis

The data required for this study was collected through semi-structured interviews which followed a conversational format where a set of predetermined questions were used in the interviews. Some questions asked spontaneously based on the nature of the conversation. The analysis for this study was conducted using a thematic analysis where the themes that emerged from the data were used to understand the experiences, thoughts and behavioural patterns that were present in the dataset.

3.2 Sample Population

The method used to identify the sample population for this study was the cluster sampling method where a group of people (adult WhatsApp users) in a specific geographical location (South Africa) were targeted and approached in their capacity as individuals to participate in this study. The study also followed the saturation approach where the number of participants for the study was not defined. Instead, interviews are conducted until a point where conducting additional interviews yielded no meaningful insights to the study (Corkum, Lohiniva, Mahoney & Wolff, 2018). Figure 2 summarizes the distribution of the sample population that was observed for this study according to age group.

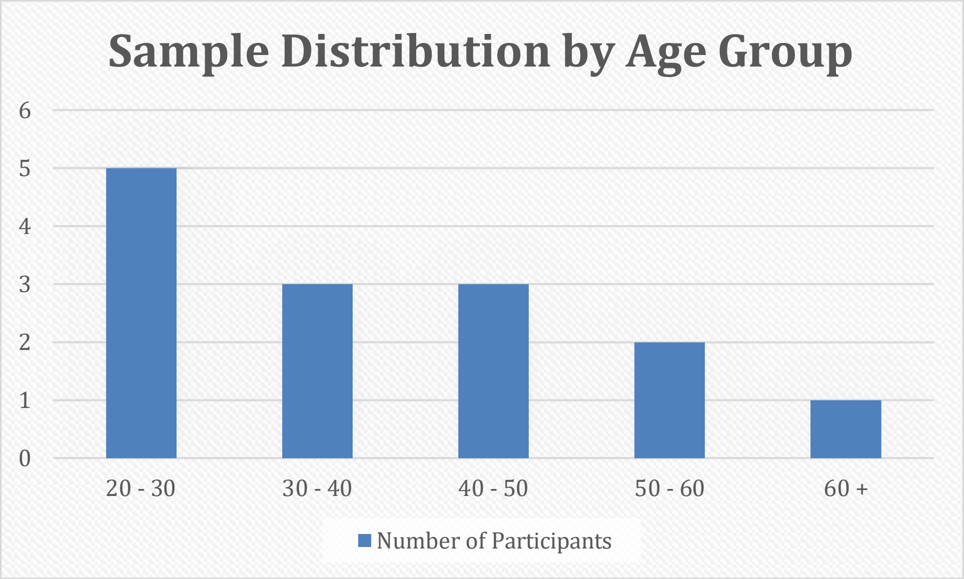

Figure 2. Sample population distribution according to age group

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

Table 1. Sample population description

4 Results

The results and major themes that emerged from the data in relation to the research objectives and questions will be presented using a method described by Cresswell (2014: 254) as the findings comparison table. The tables presented in this section will be used to represent the results where extrapolations and descriptions will be added to the comparisons for each theme.

4.1 User Awareness

The first sample comparison table compares users' answers into two categories based on whether they were aware or unaware of the policy. When looking at the theme of user awareness, it was found that users had some knowledge of the policy but not extensive knowledge of what the policy entailed or how it would impact them. In other words, though the users classified themselves using either one of the two descriptions, all users were aware of the policy. The variance in the data comes from the fact that some users were more aware of the policy because of their professional background. For example, people who had a legal or technological background appeared to understand the policy relatively more compared to users who did not. What was also discovered from the results is that users are no longer as conscious of the policy in comparison to when it was introduced in January 2021. One user confirms this by stating: "*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."* (U4).

Aware	Not Aware
"Yes, I am. I don't really know the details." ~U1	*"I know nothing about it, I just know it existed."* ~U4
"I'm aware that there was a policy that was introduced." ~U10	*"I don't know much about it affecting the business accounts."* ~U8
"I am aware of it more or less… but I didn't really read it." ~U4	*"I didn't follow (it)."* ~U13
"I found out about it from the news." ~U6	*"The deadline extension I wasn't aware of."* ~U4

Table 1. User awareness

4.2 Perceptions

The second sample comparison table looks at the theme of user perceptions and presents evidence showing what opinions users in this sample population have about the policy. These perceptions or "opinions" have been categorised into three categories namely favourable, neutral, and unfavourable opinions. In general, there were fewer positive perceptions about the policy in comparison to the neutral and negative ones. These positive perceptions mainly came from users with a legal background 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."* (U7).

The introduction of the policy caused a lot of debate and WhatsApp received a lot of criticism. However, the main perceptions from users about the policy were neutral, not unfavourable, with users stating WhatsApp's accessibility and lack of alternatives for central communication as their main reasons. One user confirms this by stating: *"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."* (U2).

Favourable	Neutral	Unfavourable
"(The policy), it is a necessary thing to have" ~U7	*"I would probably still (have) accepted, but it would have been nicer if I had the choice.*" ~U8	*"I'm not going to. I don't have any incentive to accept it."* ~U 1
"My trust level for them (WhatsApp) is much higher than these other apps…" ~U6	*"I didn't have any specific feelings, 'cause I still… don't know much about it." ~U4*	*"I'm not really happy about it… I can live without it (WhatsApp)." ~U8*
"My trust with WhatsApp is very good." ~U8	*"If I don't use WhatsApp, what am I going to use?"* ~U2	*"I feel that I'm being forced to agree to something that I'm not comfortable with." ~U12*

Table 3. User perceptions

4.3 User Reactions

The third sample comparison table looks at how users responded to the privacy policy given their knowledge and perceptions of it. In general, users accepted it but there is evidence to suggest that users accepted the policy out of necessity and not choice with one user stating: *"you have to accept it for you to continue having the platform."* (U10). Another common reaction is that users did not remember taking the time to read the policy in depth before accepting it, despite identifying themselves as privacy-conscious individuals. Lastly, even with users who have not accepted the policy, they all verified that they are still using WhatsApp because of 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 users opted for Signal. However, all users who switched stated that they were attracted back to WhatsApp because of its end-to-end encryption feature that they felt was lacking in other services.

Accepted the Policy	Did Not Accept the Policy
"I don't remember doing it. I probably did…I guess you've got to agree to it to keep using WhatsApp…" ~U3	*"(I) suppose that (at) some stage I'm going to have to accept it this. I don't really have a choice." ~U1*
"I accepted it, it prompted me for that. I accepted it." ~U6	*"I was one of the people that that was first in line to delete WhatsApp of my phone." ~U12*
"…you (have to) accept it for you to continue having the platform and because the platform is what like what we use for communication." ~U10	*"It (the policy) still comes up every now and again (but) I just ignore it because I do have an alternative, I've got Signal." ~U13*

Table 4. User reactions

4.4 Online Privacy

Based on the results presented in the first three tables, there is evidence to suggest that users' reactions to the policy were influenced to some extent by their knowledge and perceptions of the policy. There is also further evidence in the data which suggests that users' reactions were not influenced solely by those two factors. Users' attitudes regarding their respective levels of privacy consciousness also influenced how they reacted to the policy. An example of this is seen with User 1 who had a strong, negative view about the policy and thus did not accept it. In contrast, users like User 5 who had a more neutral perception about the policy were less resistant towards the policy and thus accepted it without much deliberation.

"I realised that nothing is really private" ~U4
"I wouldn't want my data to be out there" ~U1
"I am driven by privacy very much so" ~U10
"...companies were already sharing our data anyway but they're just being clearer about their intentions now". ~U2

Table 5. User perceptions about online privacy

4.5 Individual Influences

In addition to individual perceptions and behavioural patterns regarding online privacy, more individualistic factors were found to have influenced users' reactions to the policy. An example of this is seen with User 12 who is one of the older participants in this study or User 13 who understands the value of *"building a portfolio (of) consumer data"* because of her professional background in digital marketing. Both participants, however, viewed the policy unfavourably despite the contrasting individual factors described previously. It can therefore be assumed that the unique combination of a user's knowledge about, perceptions of, and attitudes towards the policy all influenced their reactions to the policy to some extent. No strong evidence was found in this sample to suggest a relationship between gender and user perceptions or reactions to the policy.

Description	**Influence/ Factor**
"I work for a retailer, so I understand marketing... and building a portfolio (of) customer data" ~U11	Professional Background
"I don't really have a high regard for Facebook" ~U1	Individual Attitudes
"I would say (I'm) just out of baby Boomer... I've been around a while, so you grew up with a lot of face to face." ~U12	Age Group/ Generation

Table 6. Individual user influences and user reactions

5 Discussion

As described in the literature, several factors influence how users respond to online privacy breaches or how they manage themselves online. There are some generic factors, with the most significant influences coming from users' unique points of reference.

5.1 Online Privacy and User Behaviour

One theme which emerged from the data that was covered extensively in the literature is that of online privacy or privacy consciousness. Privacy-conscious individuals or privacy actives were characterised by their relentlessness regarding their standards and expectations of privacy policies. If privacy actives were dissatisfied with a service, they would not hesitate to discontinue their use of said service (Redman & Waitman, 2020). Most of 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, all users, including those who had strong, negative perceptions about the policy confirmed that they are all still using WhatsApp. This behavioural pattern that was observed from users was described in the literature by Acquisiti and Gross (Acquisiti & Gross, 2006). Though users generally expressed their dissatisfaction about the policy openly, their actions did not reflect their concerns. The behavioural patterns observed in this sample population also matched those that were observed by Hess and Schreiner (Hess & Schreiner, 2015) in their 2015 study where it was found that users would rather continue their use of an online service they are generally dissatisfied with because of the social opportunity costs and networking factors involved.

5.2 Micro and Macro Economic Influences

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 (Budak et.al, 2021). The combination of users' knowledge, perceptions and attitudes about social media and online privacy influenced their reactions to some extent. These factors were described by Budak et al. (Budak et.al, 2021) as micro and macro-economic factors which would influence how resilient a user would be to an online privacy breach. Therefore, when putting the model developed by the authors in the context of this topic, the following would apply:

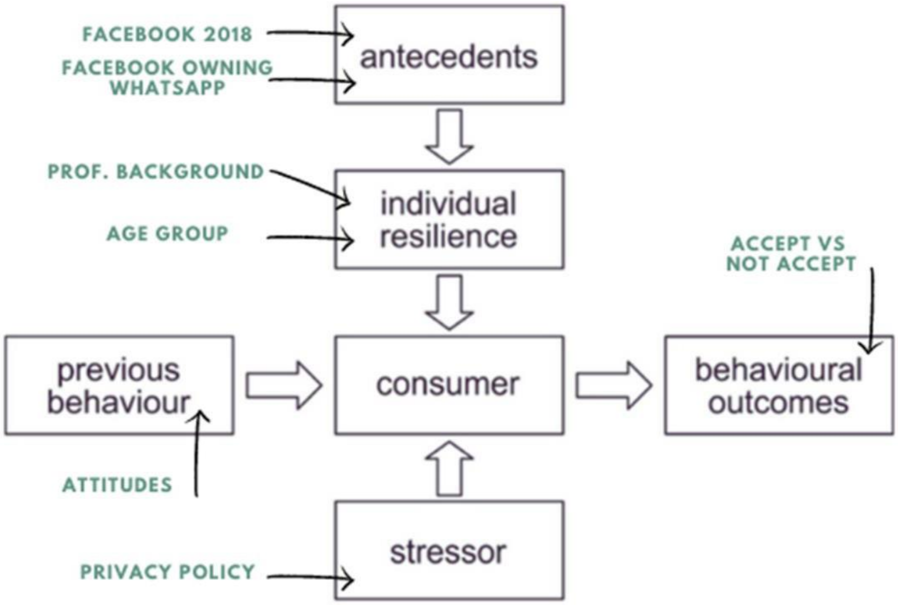

Figure 3. Updated research framework of consumer resilience to privacy violation online

The antecedents which influenced the behavioural outcomes of this population the most were users' perceptions about the 2018 Facebook-Cambridge Analytica Scandal. Some users were also further influenced by their perceptions of WhatsApp being owned by Facebook.

Individual factors such as a participant's age group and professional background also influenced users' reactions to the stressor, which in this case is the privacy policy. The combined impact of "Individual Resilience" or attitudes about internet usage and general online privacy were arguably the most significant factors that influenced users' reactions to the policy. This was observed with users whose attitudes were strongly influenced by their knowledge of prior, similar events that were also well-publicized.

6 Conclusion and Recommendations

This study has examined the social phenomenon evoked by WhatsApp's January 2021 privacy policy in a South African context. The aim was to explore what users knew about the policy, how they perceived it and how their perceptions influenced their reactions. In summary, all users knew about the policy to some extent, with most citing the news, social media and their peers as their sources of information. However, despite the overall criticism WhatsApp received when the policy was introduced, users generally had neutral perceptions about the policy and generally accepted the terms without resistance. 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. Even those who had positive or neutral perceptions about the policy expressed how they would have appreciated being given a choice. The disparity in regulations between countries has also left users to act on their own as it seems that most developing countries do not have privacy laws that are strong enough to protect their users from data surveillance perpetuated by powerful multinational corporations. Despite there being evidence of effort from some governments to regulate the policy, some countries still struggle to implement timely and effective laws to regulate the collection, processing and storage of citizens data by multinational companies.

Due to the time constraints, the long-term implications of this social phenomenon were not observed. The study was further limited by the COVID-19 pandemic which restricted the number of participants that were allowed to participate in this study. It is therefore recommended for researchers to use this study as grounds for further large-scale research that will study a similar social phenomenon from the perspective of different subjects, who might have different or similar experiences and perceptions about the same phenomenon. The insights found from different or similar sample groups can be used to help researchers, lawmakers, regulators and governments to better understand user behaviours and perceptions of social media and how to structure the relevant policy changes in response.

7 References

Acquisiti, A. & Gross, R. (2006). Imagined communities: awareness, information sharing, and privacy on the Facebook, *Proceedings of the International Workshop on Privacy Enhancing Technologies*, 4258, pp. 36 – 58. DOI: https://doi.org/10.1007/11957454_3

Adams, N. R. (2021). WhatsApp privacy concerns in South Africa explained. Available: https://mybroadband.co.za/news/security/384886-whatsapp-privacy-concerns-in-south-africa-explained.html

Ainley, P & Cohen, P. (2000). In the country of the blind? Youth studies and cultural studies in Britain, *Journal of Youth Studies*, *3*(1), pp. 79-95.DOI: https://doi.org/10.1080/136762600113059

Alhabash, S., Cotten, S.R., LaRose, R., Rifon, N.J., Shillar, R. & Tsai, H.Y.S. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behaviour*, 48, 199-207.

Baloyi, N., & Kotzé, P. (2017). Are organisations in South Africa ready to comply with personal data protection or privacy legislation and regulations? In *2017 IST-Africa Week Conference (IST-Africa)*, pp. 1-11. DOI: 10.23919/ISTAFRICA.2017.8102340

Beigi, G. (2018). Social Media and User Privacy, *Computer Science – Cryptography and Security*, Arizona State University. Available at: https://arxiv.org/pdf/1806.09786.pdf

Bhattacharjee, A. & Dana, J. (2017). *People Think Corporations Can't Do Good and Make Money. Can Companies Prove Them Wrong?* Harvard Business Review. Available: https://hbr.org/2017/11/people-think-companies-cant-do-good-and-make-money-can-companies-prove-them-wrong

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

Bonanno, E. R. (2014). The Social Media Paradox: An examination of the illusion versus the reality of social media, *The Sociological Imagination: Undergraduate Journal*, *3*(1), pp. 1 - 14.

Budak, J., Rajh, E., Slijepčević, S. & Škrinjarić, B. (2021). Conceptual Research Framework of Consumer Resillience to Privacy Violation Online, *Sustainability*, 13(3), pp. 1 – 14. DOI: https://doi.org/10.3390/sU10031238

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

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.* Springer International Publishing, London, UK, pp. 169–185. DOI: http://doi.org/10.1007/978-1-4419-6967-5

Cohen, C., Copi, I. & Flage, D. (2006). Essentials of Logic (2nd Edition), Available: https://www.ebooks.com/en-za/book/95797049/essentials-of-logic/irving-copi/?_c=11, Pearson Inc.

Corkum, M., Lohiniva, A. L., Mahoney, F. & Wolff, B. (2018). Collecting and Analyzing Qualitative Data, Available: https://www.cdc.gov/eis/field-epi-manual/chapters/Qualitative-Data.html, The Centers for Disease Control and Prevention.

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), pp. 437-446. DOI: https://doi.org/10.1111/cobi.13708

Fiesler, C. & Hallinan, B. (2018). "We Are the Product": Public Reactions to Online Data Sharing and Privacy Controversies in the Media in *Proceedings of the 2018 CHI conference on human factors in computing systems*, 53, pp. 1 – 13. DOI: https://doi.org/10.1145/3173574.3173627

Goldstuck, A. (2012). Internet matters: The quiet engine of the South African economy. *World Wide Worx, 236*.

Gruzd, A., Hernández-Garcia, A. & Jacobson, J. (2020). Social media marketing: Who is watching the watchers?, *Journal of Retailing and Consumer Services*, 53, 101774. DOI: https://doi.org/10.1016/j.jretconser.2019.03.001

Hess, T. & Schreiner, M. (2015). Examining the role of privacy in virtual migration: the case of WhatsApp and Threema, *Proceedings of the 21st Americas Conference on Information Systems*, pp. 1 – 11.

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

Kigo, M. E., & Varpio, L. (2020). Thematic analysis of qualitative data: *AMEE Guide No. 131, Medical Teacher*, 42(8), pp.846 – 854. DOI: https://doi.org/10.1080/0142159X.2020.1755030

Kwet, M. (2020). Surveillance in South Africa: From Skin Branding to Digital Colonialism in *The Cambridge Handbook of Race and Surveillance, Forthcoming*, pp. 1 – 20. Yale Law School. DOI: http://dx.doi.org/10.2139/ssrn.3677168

Limakrisna, N., Suryanti, S. & Wijoyo, H. (2021). The effect of renewal policy privacy policy whatsapp to consumer behaviour. *Insight Management Journal. 1*(2). 26-31

Lipman, R. (2015). Online Privacy and the Invisible Market for Our Data. *Penn State Law Review*, *120(3)*, pp. 777 - 806.

Perez, S. (2020). *Report: WhatsApp has seen a 40% increase in usage due to COVID-19 pandemic.* Available: https://techcrunch.com/2020/03/26/report-whatsapp-has-seen-a-40-increase-in-usage-due-to-covid-19-pandemic/, TechCrunch

Pierson, J. (2014). Online Privacy in Social Media: A Conceptual Exploration of Empowerment and Vulnerability, *Communications & Strategies*, 88(4), pp. 99 -120.

Rajpurohit, G. S. & Yadav, R. K. (2021). A Socio-Legal Analysis of WhatsApp Privacy Policy 2021 in India: A Contemporary Study, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3850579. DOI: http://dx.doi.org/10.2139/ssrn.3850579

Redman, T.C. & Waitman, R.M. (2020). *Do You Care About Privacy as Much as Your Customers Do?* Available: Do You Care About Privacy as Much as Your Customers Do? (hbr.org), Harvard Business Review, Harvard Business Review.

Singh, M. (2021). *WhatsApp details what will happen to users who don't agree to privacy changes,* Available: https://techcrunch.com/2021/02/19/whatsapp-details-what-will-happen-to-users-who-dont-agree-to-privacy-changes/, TechCrunch

Shambare, R. (2014). The Adoption of WhatsApp: Breaking the Vicious Cycle of Technological Poverty in South Africa, *Journal of Economics and Behavioural Studies*, 6(7), pp. 542 – 550. DOI: https://doi.org/10.22610/jebs.v6i7.515

Somari, D. (2021). *What will happen if I do not accept WhatsApp New Privacy Policy?* GadgetsNow. What will happen if I do not accept WhatsApp New Privacy Policy? - Times of India (gadgetsnow.com)

WhatsApp.com. (2021). *WhatsApp Privacy Policy (Last modified January 04, 2021).* Privacy Policy (whatsapp.com)

Zuboff, S. (2019). Surveillance Capitalism and the Challenge of Collective Action, *SAGE Journals,* 28(1), pp. 10 – 19. DOI: https://doi.org/10.1177/1095796018819461