

Ignorance or Inaction: An Analysis of Social Media Users' Perspective on Privacy in Data Collection. A Study of Tertiary Students in the Greater Accra Region of Ghana

¹Modestus Fosu  ²Martin Thompson Kwadzo Ntem  ³Wise Kwame Osei 

^{1,2,3}University of Media, Arts and Communication-
Institute of Journalism, Accra

Corresponding author: Modestus Fosu, Email: mfosu@unimac.edu.gh

<https://doi.org/10.63772/jocmas.v11n1.3>

Abstract

This study focuses on tertiary education students in Ghana and investigates their awareness, perspectives, and behaviours regarding data and privacy on social media. Little research has examined whether Ghanaian tertiary students' social media data privacy behaviours stem from strategic awareness, ignorance, or carelessness. Grounded in Uses and Gratifications and Privacy Paradox theories, this qualitative study explores awareness patterns, data protection strategies, and factors that influence the ongoing disclosure of personal information on online platforms. Data were drawn from focus group sessions involving students from the University of Media, Arts and Communication (UniMAC), the University of Ghana (UG), and the African University College of Communication (AUCC). It was found that social media users in tertiary schools engage in a complex interplay of awareness, utility, gratification, and risk management regarding data protection on social media. This indicates that online data protection behaviours stem from cognitive processes that compromise utility and gratification, rather than mere carelessness and inaction. These findings underscore the need for improved data protection education among students and the reassessment of online data protection regulations in Ghana.

Keywords: *Online privacy, data protection online, social media, tertiary students, Privacy Paradox Theory, Ghana*

Submitted: 11th March 2026

Revised: 22nd June 2026

Accepted: 16th September 2026



Introduction

The proliferation of social media platforms and their use have radically transformed interpersonal communication, content sharing, and social relationships globally (Meral, 2021; Whiting & Williams, 2013). Social life is rapidly transitioning to online platforms, encompassing both User-Generated Content (UGCs) websites, such as YouTube and Wikipedia and Social Network Sites (SNSs), including Facebook, Instagram, Twitter, and TikTok (Custers et al., 2014; Trifiro, 2022). To function, these online platforms rely on users sharing personal data, such as names, email addresses, phone numbers, photos, locations, interests, and more. Beyond registration data, analytics can continuously track online behaviour across platforms to generate insights (Kokolakis, 2017). This underscores legitimate concerns about the privacy and appropriate exploitation of users' voluntarily provided information that can be tracked during platform engagement (Ciftci et al., 2023). The apparent uncertainty about how personal data are utilised connects with issues of protection and privacy on social media (Beigi & Liu, 2020).

The sheer magnitude of personal data generated, coupled with significant reductions in the cost of data storage and analysis, has naturally given rise to profound privacy concerns among the general public and policymakers. Social media network providers are deliberate and selective in the personal information they require users to supply before using their platforms. Users are often required to provide personal information such as their gender, email addresses, contact information, medical information, educational records, financial and credit card information, and information concerning ethnicity and race. (Jain & Sahoo, 2021). Details of social media usage and the types of content users often consume, or in some instances would like to consume, are also required (Aljohani et al., 2016; Tuunainen et al., 2016; Beigi & Liu, 2020). The expanding scope of online social and economic activities, ranging from sharing location data on Uber to seeking medical information or diagnoses on Google, generates copious data. While data are harnessed to enhance products and services for consumers, the negative implications are real and not assumed (Vgena et al., 2022). Examples such as Cambridge Analytica's use of Facebook data to influence election outcomes and manipulate public opinion, or health insurance companies predicting the medical needs of potential policyholders based on undisclosed personal data, underscore the widespread opportunities to exploit user data (Hinds et al., 2020). These and other privacy scandals and data breaches in recent years have heightened concerns regarding consumer privacy (Markos et al., 2023). Consequently, data privacy has emerged as one of the most significant challenges facing the global digital economy. Although governments have responded with new data privacy laws and regulations, scholars such as Lie et al. (2022) argue that these measures are only partially effective.

Researchers (Shao et al., 2022; Alzaidi & Agag, 2022) have raised crucial questions about whether users are sufficiently informed of the consequences of sharing their personal information online. These questions often focus on the availability, accessibility, and user-friendliness of platform policies, regulations, and data security measures, placing responsibility on service providers for users' insufficient information about their data security. We contend that, in addition to user awareness, it is necessary to investigate how social media users proactively safeguard their

privacy. This includes whether they consciously explore platform tools and other mechanisms to limit tracking and data breaches or are careful when sharing sensitive information online. Nevertheless, research examining users' adoption of available privacy controls remains limited, particularly in Africa. Existing studies have explored users' adoption of privacy controls, their intentional adjustment of privacy settings for online self-protection, and the factors influencing their willingness to voluntarily disclose personal information (Wisniewski et al., 2017).

The matter is complicated by the fact that the Internet has created seamless spaces intimately connected with people's lived experiences, underscoring the relevance of this study. Recent studies on algorithmic governance, datafication, and platform economies have demonstrated various opportunities, threats, and usability in contemporary digital spaces, emphasising the ethical and protection issues underlying being online (Donald et al., 2023; European Parliamentary Research Services, 2019; Latzer & Festic, 2019). These studies also indicate that decision-making processes in people's daily lives have potentially important implications for individuals, organisations, and societies. These findings are particularly concerning in Africa because youth, who make up the majority of citizens, are constantly seeking opportunities and self-expression online (Latzer & Festic, 2019). These issues require investigation to find solutions that empower online users to control their data, particularly in Africa.

Several studies have examined social media privacy in Ghana. Owusu et al. (2020) focused on the continued use of mobile social media amid privacy concerns, revealing that hedonistic factors, such as perceived usefulness, enjoyment, trust, and ignorance of privacy issues, could account for the continued use of applications. Other studies have highlighted the negative or harmful aspects of social media use (Atiso & Kammer, 2018). Such studies identify avenues through which cybercriminals can perpetrate scams, hacking, or other forms of fraud and infringe on people's rights by invading their privacy, damaging their reputation, and engaging in blackmail.

A critical gap in the existing literature on Ghana concerns the little focus on tertiary-level students' personal motivations, understanding of online risks, and their decisions and actions regarding platform use. Although Boateng (2022) notes that tertiary students form a large body of heavy social media users in Ghana, few studies have engaged this issue from the perspective of university students. However, scholars such as Taddicken (2014) have acknowledged students' intensive use of online platforms, which exposes them to the data collection and surveillance activities of social media service providers. Students' regular activities, such as sharing, posting, liking, and commenting on social media platforms, generate important data beyond personal information that service providers exploit (Kokolakis, 2017). Nonetheless, little is known about the strategies tertiary students adopt to protect their data from service providers and other social media users, thereby limiting understanding of students' attitudes and behaviours towards data use and privacy on social media. The crucial issue is the extent to which students in Ghana are aware of the scale of the data they provide, and the risks involved in providing their information online. The assumption is that they could (in)advertently authorise the collection or (mis)use of their sensitive details.

Thus, this study aimed to investigate Ghanaian tertiary students' perspectives on their knowledge and actions regarding data and privacy on social media. The following are research questions the study seeks to address:

- To what extent are tertiary students in Ghana aware of the collection and use of their personal information when they sign up to use social media?
- How do tertiary students safeguard their personal data on social media applications?
- What factors influence students to provide personal information despite their awareness of its collection and use by service providers?

This study provides valuable insights into tertiary-level students' digital literacy inclinations and their attitudes toward issues involving their online data. The findings could provide a useful index of the many young people at non-tertiary levels in Ghana and across Africa who are increasingly accessing online platforms in an era of greater technological access and penetration.

Privacy policy concerns in social media use

Issues of online privacy literacy and privacy management have attracted research attention. According to Gerber et al. (2018), users tend to underestimate privacy risks, possibly because they have not personally experienced the negative effects of privacy violations. In the context of social media, a privacy policy outlines a platform's policies for gathering, using, sharing, and safeguarding user privacy, thereby acting as a legal framework for user-platform interactions and providing transparency on data management procedures and privacy protections. Social networking platforms may have different privacy policies, but they usually cover several important matters, such as data acquisition, the types of information that the platform collects from its users, and information gathered via users' interactions, such as postings, comments, and location data, in addition to the data supplied during the registration process (Ur et al., 2012).

The policies address users' data use and content sharing, clarify how user data is used and distributed, and indicate how social media platforms exploit such data to improve user experience, customise content, and show relevant advertisements. Crucially, the policies also clarify how user data may be shared with external parties, emphasising the importance of user agreements in such situations (Yang et al., 2015). Scholars have highlighted data security as a key aspect of privacy policies to protect user data from abuse, breaches, and illegal access, including through authentication and encryption (Das et al., 2018; Kuczerawy & Coudert, 2011). According to Such and Rovatsos (2016), privacy policies also disclose users' access and control rights, including the power to examine, amend, or remove their personal data and to adjust privacy settings to suit their tastes and comfort levels (Kumar et al., 2016). These policies cover how cookies and tracking technologies are used and how user data are gathered and analysed using various technologies to enhance services, customise user experiences, and enable targeted advertising. Thus, policies aim to offer users transparency (Jozani et al., 2020; Petersen & Lehmann, 2018), empowerment (Wu et al., 2010), and control over personal online information by emphasising legal rights and options for managing data.

However, privacy policies also pose challenges (Meier et al., 2020). Policies are not only dynamic with regular revisions that leave users behind, but are also often presented in linguistically complex language, which scholars argue could make them difficult to read and understand (Fosu, 2016). Thus, users carry the burden of constantly making a conscious effort to be abreast of the specific information and demands of the policies and adjust accordingly. Human frailty and the urgency to access social media sites to satisfy cravings mean users cannot always review these policies before accessing platforms each time.

Opinions in the literature on social media privacy are divided about the degree to which social media users are concerned about their privacy and the data acquisition techniques adopted by service providers. While some studies have found that users rarely concern themselves with these issues (Litt, 2013; Litt & Hargittai, 2014), others have indicated otherwise (Wu et al., 2010; Singh, 2021; Ibdah et al., 2016). Some studies have found that a significant proportion of social media users are indifferent to service providers using their information (Fernandes & Pereira, 2021; Litt & Hargittai, 2014). According to Litt (2013) and Litt and Hargittai (2014), social media users often disclose personal information, grant extensive platform permissions, and rarely use privacy protection protocols, suggesting a lack of concern for their privacy. Other studies have noted users' concerns about how service providers use their (users) data. In the USA, for instance, McClain et al. (2023) found that many social media users expressed anxiety and distrust and recommended stronger data regulations.

Other studies have found that some social media users express concern about the use of their private information but still engage in behaviours that suggest indifference to those concerns. For example, Fernandes and Pereira (2021) and Norberg et al. (2007) noted a measurable divergence between individuals' stated disclosure intentions and their actual behaviour. Kokolakis (2017) found that many people report moderate to high privacy concerns but show inconsistent privacy behaviours. Various reasons may account for this. Krasnova et al. (2010) argue that when the perceived immediate social or instrumental benefit outweighs abstract future harm, users are likely to disclose information despite their concerns. Brandimarte et al. (2013) argue that users often face complex technical privacy choices and lack the time or expertise to assess long-term risks, leading them to engage in risky privacy disclosure. In effect, the disclosure of private information on social media and users' awareness of how such data is used form a complex web of paradoxical intention-behaviour interactions: while users may be concerned about the use of their private information, they still engage in risky disclosure behaviours on social media platforms.

Studies have found similar insights among students who, by virtue of being students, are deemed to be knowledgeable about social media use (Krasnova et al., 2010; Lewis et al., 2008; Salleh et al., 2013). Rafique (2017) and Aboulnasr et al. (2021) found that, despite privacy concerns, students disclosed large amounts of personal information, often driven by convenience and other factors. Krasnova et al. (2010) attributed this, debatably, to trust in national data-protection regulations, although this may be highly contested today, especially in Africa. These studies typify the extent of students' knowledge of personal disclosures, the associated risks, and the paradox

therein. In other words, the literature strongly suggests that while social media users may be aware of the data collection and use practices of social media service providers, they are often not apathetic about disclosing their personal information. The discussion in this section and the findings relate to non-African jurisdictions, raising questions about whether Africa shows similar trends.

Theoretical Framework

This study's analysis is underpinned by the Uses and Gratifications Theory and Privacy Paradox Theory. These theories represent a mix of theoretical perspectives from psychology, sociology, communication, and information systems to provide an insightful understanding of the motivations and inclinations underlying the issues of this study. Thus, although fraught with some limitations (Zuboff, 2019; Susser, Roessler, & Nissenbaum, 2019; Acquisti et al., 2015), they provide adequate analytical rigor to guide the analysis.

Uses and Gratifications Theory

Uses and Gratifications Theory (UGT) explains how individuals actively choose and use media to fulfil specific needs and desires. This communication theory, developed by Katz et al. (1974), argues that people are not passive consumers of media but actively select, interpret, and derive gratification from media content. The theory emphasises the active role of individuals in selecting and using media to fulfil specific personal needs, such as information-seeking, entertainment, social interaction and identity construction (Katz et al., 1974; Heravi et al., 2018). This orientation is critical for understanding the relationships and dynamics among social media users, online service providers, online data provision and use, and privacy issues. As Quan-Haase and Young (2014) observed, online platforms serve as arenas in which users actively construct and express identities, build relationships, and seek affirmation. Yet, while users perceive themselves as autonomous agents deriving satisfaction from these interactions, their engagement simultaneously exposes them to sophisticated forms of data surveillance and the commodification of personal information (Zuboff, 2019). This paradox underscores a critical tension inherent in UGT and applicable to the current study: the gratifications users seek and the implications for their online privacy and welfare.

Privacy Paradox Theory

The Privacy Paradox Theory (Norberg, Horne and Horne, 2007) offers a critical perspective for understanding user behaviour in the context of privacy and data collection on social media platforms. The theory highlights the complex and often contradictory psychological tendencies social media users exhibit when accessing online sites (Kokolakis, 2017), where users express concerns about their online privacy but continue engaging in activities that compromise it. The theory suggests factors that contribute to this paradox, one key factor being the convenience and benefits of online services and social media, which often require disclosing personal information (Barrett-Maitland & Lynch, 2020). Social media platforms are structured to maximise user engagement by offering personalised services, algorithmically curated content, and social validation mechanisms, which subtly encourage sharing personal information despite known privacy risks (Chen, 2018). Users may prioritise the immediate benefits of these services over privacy concerns (Kokolakis, 2017). Thus, the theory provides analytical insights into tertiary

students' expressed concerns about online privacy and their behaviour on social media platforms in Ghana.

Methodology

This study adopted a qualitative approach, using phenomenology (Creswell & Poth, 2018) to explore social media users' lived experiences and perceptions of data collection privacy on social media platforms (Manen & Manen, 2021). Data were collected from students at three public universities in Ghana: The University of Media, Arts, and Communications (UniMAC), the University of Ghana (UG), and the African University College of Communication (AUCC), all in the Greater Accra region. These universities have strong departments hosting media and communication programmes and courses, making them appropriate data sites for this study. The assumption is that students in such departments should be savvy about online privacy implications. Apeanti and Essel (2021) argued that tertiary students constitute a relevant population for examining social media users' perspectives on online privacy, as they are likely to be active users of social media platforms and can provide valuable insights into the subject matter. Overall, 30 participants were purposively selected across the three universities, comprising two registered students from each level of study (ranging from first- to final-year undergraduate to master's level), totalling 10 students per university. This number balances the need for depth in qualitative research with the practical constraints of data collection, saturation, and analysis (Hennink & Kaiser, 2021).

Data were collected using semi-structured interviews and focus group discussions (FGD) from September to November 2023 at the universities. Each FGD included 10 participants from one university, and the discussion took place in a conducive environment that facilitated active participation (Barbour, 2007). These two data collection approaches enabled the collection of relevant data that considered the participants' perceptions, attitudes, and experiences through interactive dialogues, yielding diverse meanings and shared experiences within social contexts, which are crucial when studying social media users (Krueger & Casey, 2015). Before data collection began, participants received and completed informed consent forms outlining the study's objectives, emphasising the voluntary nature of their participation, and assuring them of strict confidentiality for their identities and responses.

The interview and FGD responses were audio-recorded and manually transcribed by a trained research assistant. One author reviewed the transcriptions to ensure accuracy. In line with the study's qualitative orientation, two authors inductively open-coded the data to generate contextualised themes that were interpretive and amenable to socially mediated meanings for each research question (RQ). Themes for RQ1 were awareness and knowledge of privacy policies. RQ2 focused on passwords and verification, privacy settings, and incorrect information, while RQ3 focused on security assurance and access. The data were then analysed and presented according to these themes. The third author cross-checked the codes and themes to ensure the process was trustworthy. Following Braun and Clarke (2021), the data were then analysed inductively according to these themes under the various RQs. The results are presented in a descriptive narrative supported by copious quotes from the data, as expected in a qualitative study.

Results and Discussion

This section presents and discusses the study's findings in relation to the research questions. The first part presents and discusses the participants' social media preferences, followed by a focused analysis and discussion of the research questions.

Awareness of online data collection: Social media apps are used frequently

One issue this research sought to uncover was which social media applications participants regularly used to infer their social media preferences. The findings revealed varied preferences among the respondents, offering insights into their social media usage habits. Facebook emerged as the most used platform, with all the participants reporting regular use. This finding supports existing literature that Facebook remains the most used social media platform in Ghana, followed by WhatsApp, Instagram, X (formerly Twitter), TikTok, YouTube, and Snapchat. The respondents' differing preferences support the relevance of the Uses and Gratifications theory underpinning this study. Katz, Gurevitch, and Blumler (1974) note that the theory explains media consumers' preferences and the motivations behind them.

RQ1: To what extent are tertiary students in Ghana aware of the collection and use of their personal information when they sign up to use social media applications?

The first research question explored tertiary students' awareness of social media service providers' data collection and use practices. This section explores students' awareness of the practices and assesses their knowledge of the data privacy policies of the social media apps they use.

Awareness of data collection on social media apps

The analysis revealed mixed reactions to respondents' awareness of social media applications' data collection practices. Nonetheless, a significant majority of respondents said they knew their personal information was collected when they registered for and used these platforms, while a few participants said they were unaware.

Yeah, many times, they ask for your personal details, which should be private (ST14, Male, 27 years).

This finding aligns with existing research that a significant proportion of social media users are aware that by signing on to social media platforms, they disclose their personal information (Eveleth & Eveleth, 2021; Custers et al., 2013). This finding suggests that, while aware of the collection of their personal data, respondents also know their data could be used for other purposes by the social media service provider. For the few participants who were ignorant about the possible invasion of their privacy, Beck et al. (2021) and Quinn (2016) acknowledge that while this may be common among social media users, the nature of privacy warnings on social media platforms, as well as the levels of digital media literacy of social media users, have critical implications for their awareness of data collection tendencies.

Knowledge of Privacy Policies: Reading the privacy policies of social media apps

This study investigated whether respondents read privacy policies to gauge their knowledge of online privacy issues. The study found that social media users have little knowledge of specific privacy issues and policies on social media platforms because they rarely read privacy policies. The study found that this behaviour was prevalent among social media users who perceived the policies as irrelevant. One respondent stated:

No, because I don't see it as important (ST003, Female, 19 years).

This perspective highlights a prevailing sentiment among some users who do not consider reading these policies a priority or necessary practice, thereby exposing a critical gap between user awareness of data collection and their actual engagement with privacy-related information. Thus, although participants generally acknowledged that they were aware and concerned about how their personal data were collected and used, few demonstrated proactive behaviour in knowing the details of privacy agreements. This behavioural pattern aligns with the privacy paradox, which describes privacy concerns alongside behaviours that expose users to privacy risks (Barth & de Jong, 2017). Furthermore, the findings align with the core tenets of Uses and Gratifications theory. That a few users spend quality time reading privacy policies on social media platforms is revealing. For users, reading privacy policies offers little gratification, as it tends to delay access to desired social interactions and impose cognitive burdens. As such, users prioritise gratification from use over the precautionary benefit of privacy awareness and action (Smock et al., 2011).

This finding underscores a broader challenge in public communication: users encounter long, complex privacy policies that are difficult to read and understand (Fosu, 2016). Many individuals may not fully grasp the potential risks associated with their online activities or the rights and responsibilities they agree with when using social media platforms (Beck et al., 2021). The findings emphasise the need for social media platforms and regulatory authorities to use simple and clear language to make the policies more accessible to users of all ages.

It is noteworthy that a few respondents were concerned about privacy issues regarding the social media they used and tried to read some of the privacy policies, as explained by one respondent:

Yes, to make sure my phone doesn't have an app or something it's not supposed to have (ST007, Female, 24 years).

This motivation for reading privacy policies was grounded in a good understanding of the potential risks of using apps and a desire to avoid unauthorised or malicious software. This supports Thomas and Gupta (2021) that people weigh benefits against risks and costs, as explained by Social Exchange Theory. These findings corroborate the Privacy Calculus theory, which posits that people are often careful about sharing information about themselves on digital media platforms (Wang et al., 2016).

RQ2: How do tertiary students safeguard their personal data on social media applications?

The data indicate that social media users have made some efforts to protect their personal information. The findings show that respondents often used passwords and verification strategies and provided false information to protect their personal information. This reflects an awareness of privacy risks and illustrates students' efforts to ensure control over their digital information.

Passwords and Verification

The data showed that participants used complex passwords and user verification approaches to safeguard their online security. To ensure passwords are effective, respondents adopted two-step verification and end-to-end encryption strategies to protect their personal data. In the extract below, one respondent described using passwords and locks to protect their personal information while using social media applications.

I do some kind of two-step verification by using passwords and locks (ST019, Female, 19 years).

Thus, users employ deliberate strategies to protect their personal data on online platforms because of the benefits they derive from using these platforms (Smock et al., 2011).

Privacy Settings

The study found that one core way respondents protected their personal data was through privacy settings. The study found that some respondents altered their privacy settings on social media apps to restrict or protect their personal information while using the apps.

I make sure to review and adjust my privacy settings regularly (ST023, Female, 26 years).

I make sure I do all the security setups (ST028, Female, 28 years).

This rational behaviour implies that social media users actively try to control data disclosure on these platforms. Key indicators included changing privacy settings, restricting app permissions, and blocking location-tracking features.

I've made sure my location is always off. I only give permission to apps that need my location for important purposes like courier services. I have also set my phone to not allow

any website to track me. When I post on Facebook, I don't add my exact location (ST016, Female, 26 years).

Yes, I have adjusted my privacy settings. I made my account private so only people I can approve can see my post, and I limited who can comment and tag me (ST009, Male, 27 years).

Tertiary students' manipulation of privacy settings indicates that they are not entirely passive and that awareness of data collection by service providers may inform such proactive cognitive behaviours. This aligns with Stutzman and Hartzog (2012), who found that students actively participate in privacy management. This proactive engagement emphasises the Uses and Gratifications Theory, which holds that users' privacy-related actions are shaped by motivations for using social media (Katz et al., 1974). In this case, privacy settings allow students to satisfy their need for social connections without compromising their desire for security.

Provision of Wrongful Information

The study found that another strategy users adopted when providing personal data online was to provide incorrect information. According to some respondents, this was necessary because providing some form of data while using social media is often a requisite for accessing some platforms:

I sometimes give out wrong information (ST011, Female, 21 years).

... I hide some vital information (ST014, Male, 27 years).

Hoofnagle et al. (2010), Taddicken (2014), Bruh et al. (2017), and others noted that this strategy is common among social media users. While Hoofnagle et al. (2010) conceptualised this as *privacy pragmatism*, in which users maintain privacy boundaries, Taddicken (2014) and Baruh et al. (2017) suggested that this behaviour offers users some degree of perceived control over their personal data online. This finding also suggests that students do not trust service providers' data collection and use practices (Smock et al., 2011). The privacy paradox theory captures students' willingness to continue using social media despite mistrust of service providers, highlighting the tension between privacy concerns and continued online engagement.

Overall, the three core strategies illustrated here underscore tertiary students' privacy-protective strategies. The findings show that these strategies are selective, pragmatic, and adaptive, reflecting both students' awareness and ambivalent behaviours towards the issues under discussion. That is, users act to protect themselves and exercise perceived control while balancing the desire for

privacy with the desire to maintain social connections through social media platforms, as suggested by the theories of gratifications and the privacy paradox.

RQ3: What key factors influence students to provide personal information despite awareness of collection and use by service providers?

This study further explored the fundamental issues that contributed to the continued provision of personal data despite the apparent knowledge of its collection and use by service providers. The study found that both functional and intrinsic factors accounted for this.

Assurance of Security

Regarding the motivational factors driving social media users to provide personal information and data on social media platforms, assurance of security was a key factor. Some respondents believed they were driven to provide personal information when service providers assured them of the safety of their data.

When there is the assurance of safety (ST003, Male, 26 years).

If I know the platform has robust security measures, transparent about data usage, and gives me control over my info, I would be more willing to share. For WhatsApp, knowing that my chats are end-to-end encrypted already helps. (ST009, Male, 31 years).

Thus, some respondents believed a critical factor in their decision to provide personal information was the security of the social media apps' privacy policies. This implies that users may avoid apps or use mitigation strategies to avoid disclosing information they do not want to share.

The study further found that assurances of data safety on social media platforms had critical implications for respondents' perceptions of service providers' transparency. Some respondents noted that assurances about the safety of personal data indicated how transparent app creators were and did not imply malice on their part. One respondent noted that transparency about how private data are kept secure may shape how much personal data people provide to these apps.

I am assured when there's transparency in the terms and conditions (ST029, Female, 25 years).

These findings align with earlier work by Barth and de Jong (2017) and Kokolakis (2017), who noted that users' trust in technological protection mechanisms often reduces privacy anxiety, even when that trust is not grounded in full comprehension of how data protection systems operate. Beyond this, the finding reflects perceived trust and control, both critical aspects of Uses and Gratifications and Privacy Paradox theories (Norberg et al., 2007).

Access to the Functionalities of the Apps

The study also found that participants continued to disclose personal information because they wanted to use certain social media applications. Thus, they provided personal information because the platforms required it to use them. Therefore, participants decided to provide such information, although they were aware of the risks involved:

... Just to get easy access and do what I want on that platform (ST018, Male, 28 years).

... To be allowed access (ST006, Female, 26 years).

This finding aligns with the privacy paradox theory and the privacy fatigue concept (Rafique, 2017; Kokolakis, 2017; Boateng, 2022), which explain how social media users are likely to provide their personal information to be able to use platforms, or because users are overwhelmed by the processes of engaging in activities that provide them with added security. While students exhibit awareness and concerns about data privacy, continued disclosure reflects behaviours shaped by trust and perceived control. Thus, students are not simply careless or ignorant of data concerns but rather engage in a complex web of negotiations between control, utility, and trust. This study reveals how user agency in media consumption is entangled with corporate strategies of data extraction. While users perceive their actions as autonomous and gratifying, platform architecture often shapes and directs these choices to maximise data capture. Therefore, privacy concerns in social media are not merely about user awareness but are deeply embedded in the gratifications platforms strategically offer to sustain user engagement and data flow.

Discussion

This study is motivated by gaps and questions in the literature (for example, Owusu et al., 2020) on data privacy on social media in Ghana. Beyond that, social media users struggle to resist the urge to stay online despite privacy concerns. Is it simply the pleasure of being online, or are users unaware of the risks they face? If users are aware, are they adequately informed about the risks their personal data faces online, or do they know but remain careless? This study aimed to untangle these perplexing issues.

The relevance of this study is underscored by the expanding implications of digital platforms beyond entertainment and interpersonal communication. The European Parliamentary Research

Services (2019) noted that algorithmic systems increasingly facilitate decision-making in people's daily lives. The implications of algorithmic governance for different groups, especially youth in Africa, cannot be overstated (Latzer & Festic, 2019). This aligns with platform economies, where datafication (Donald et al., 2023) helps businesses, governments, and individuals benefit from the growing superhighway of data in the global digital economy, which also brings digital risks. According to Latzer and Festic (2019, p.6), internet-based algorithm governance goes beyond the exercise of digital security to indicate life routines that cover people's everyday activities in the areas of "(a) social and political orientation, (b) recreation, (c) commercial transactions, and (d) socialising", among others. These benefits may account for many of this study's findings, especially the specific factors driving users' willingness to provide personal details voluntarily online, with or without knowledge of the implications (Christofides et al., 2012),

Overall, this study highlights varying levels of knowledge among social media users about privacy issues across platforms. The findings provide critical insights into how student social media users perceive social media privacy issues and whether their online privacy behaviours stem from ignorance or apathy. First, while most students demonstrated awareness of the collection and use of their personal information for good or bad purposes, most did not read privacy policies meant to safeguard their lives online. This suggests that their inaction is less a result of ignorance and more a reflection of cognitive disengagement. Second, the study concludes that users' adoption of complex strategies and behaviours to protect their personal information indicates a non-passive, intentional effort to exercise control over their desire to be online. This suggests that users are conscious of their personal information and what happens to its online usage. Thus, the various complex strategies adopted to safeguard personal data are representations of adaptive strategies influenced by platform functionalities and data protection policies.

A significant aspect of this study focused on understanding why students disclose personal data despite being aware of and concerned about their online safety. The study found that assurance of protection and the functionalities of these platforms influence continued disclosure of personal data. The study concludes that users often prioritise their desire to use social media platforms over data protection. Hence, users prioritise the gratification of social connections and interactions over abstract risk. This illustrates goal-oriented logic within the nexus of social media use and data protection.

Although privacy policies formally outline how user data are handled and used, this study reveals that some users do not understand platform data policies, extending Christofides et al.'s (2012) findings to the Ghanaian context. Research continues to highlight the belief that some users seldom read or comprehend policies because of the technical language and legalese in which they are written. The inordinate length and high content density of the policies, combined with the small font size (Obar & Oeldorf-Hirsch, 2020), challenge users' concentration, attention span, and understanding.

Thus, the analysis provides an enduring understanding of how users relate to social media platforms, the language of the policies, and the risks involved, producing a complex web of interests. Service providers would want to profit from establishing social media platforms and selling users' data to third parties. To avoid legal liability, service providers create policies and procedures that govern platform operations and outline stakeholders' responsibilities and potential uses of users' data. This may explain why the policies are long and legally oriented. Users, on the other hand, always have a compelling urge to be on the platforms. Thus, in most cases, they are unable to carefully and exhaustively read platform policies to make an informed decision about whether to sign up for the platform. They may have partial or no awareness since they may not meticulously imbibe the policies, even if they are aware of the risks. This study suggests that it is currently too simplistic to be definitive about users' online behaviours regarding their knowledge, online protection, and the disclosure of their personal data.

Conclusion

This study contributes original knowledge about the tensions and negotiations that characterise tertiary students' attitudes and orientation towards providing their personal information on social media sites to use these platforms. This study thus adds to the global literature by providing a Ghanaian perspective on this topical issue, given that the online space is fast becoming a controversial arena for harnessing opportunities and for exploitative and criminal tendencies. While online privacy and data security have been global concerns, this study appears to be one of the few to examine them from an exclusively Ghanaian students' perspective, particularly by integrating Uses and Gratifications and Privacy Paradox theories as the analytical lens. As the analysis shows, the study's findings confirm existing research, whose empirical strength hinges on heterogeneous participants. Thus, this study extends the existing literature and the theories that guided the analysis by focusing exclusively on university students who are digitally savvy and active on social media. This theoretical contribution should open space for more studies that focus on the urban-rural dichotomy and use other data sources, such as users who are not current university students.

The findings and conclusions also invite important structural, functional, and policy proposals. The finding that online privacy policies are written in complicated language that could discourage people from reading, understanding, and exploring data security measures should be concerning. This finding should prompt service providers to present such policies in simple, user-friendly language to encourage proactive user security behaviours. The finding that students' online privacy behaviours are an embodiment of rational and yet paradoxical negotiations between the desire to gratify social connections and interactions and the fear of data exploitation reveals that such behaviours may not merely imply the users' strategic awareness, ignorance, or carelessness, but a more complicated case-by-case response to the need to be online. The study's major conclusion that students' privacy behaviours emerge from a complex interplay of awareness, perceived benefit, and compromise rather than pure ignorance or carelessness is instructive and useful. It calls for government policy intervention in Africa to ensure that both users and service providers become responsible and adopt secure, ethical behaviours in digital spaces. Ghana and other African countries may consider including digital literacy in school curricula, from basic to

university, and integrating such policies into teaching and learning because social media has become part of people's everyday lives.

Declarations

AI use: The authors report no use of generative AI in the preparation of this manuscript.

Conflict of interest: The authors report no conflict of interest.

Funding: The authors received no specific funding for this work.

References

Aboulnasr, K., Tran, G. A., & Park, T. (2021). Personal information disclosure on social networking sites. *Psychology & Marketing*. 39(2), 294–308. <https://doi.org/10.1002/mar.21595>

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behaviour in the age of information. *Science*. 347(6221), 509–514. <https://doi.org/10.1126/science.aaa1465>

Aljohani, M., Nisbet, A., & Blincoe, K. (2016). A survey of social media users' privacy settings & information disclosure. In M. Johnstone (Ed.), *Proceedings of the 14th Australian Information Security Management Conference* (pp. 67–75). Edith Cowan University.

Alzaidi, M. S., & Agag, G. (2022). The role of trust and privacy concerns in using social media for retail services: The moderating role of COVID-19. *Journal of retailing and consumer services*. 68, Article 103042. <https://doi.org/10.1016/j.jretconser.2022.103042>

Apeanti, W., & Essel, D. (2021). Students' use of social media in higher education in Ghana. *International journal of multidisciplinary research and development*. 8(3), 1–12.

Atiso, K., & Kammer, J. (2018). User beware: Determining vulnerability in social media platforms

for users in Ghana. *Library Philosophy and Practice*, Article 1812.

Barbour, R. (2007). *Doing focus groups*. SAGE Publications.

Barrett-Maitland, N., & Lynch, J. (2020). Social media, ethics, and the privacy paradox. In: Cross, M. (Ed.). *Security and privacy from a legal, ethical, and technical perspective* (pp. 49–64). IntechOpen. <https://doi.org/10.5772/intechopen.90480>

- Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behaviour – A systematic literature review. *Telematics and informatics*. 34(7), 1038–1058. <https://doi.org/10.1016/j.tele.2017.04.013>
- Baruh, L., Secinta, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytic review. *Journal of communication*. 67(1), 26–53. <https://doi.org/10.1111/jcom.12276>
- Beck, E., Ellen, G. M., Ho, A., Parks, A., & Rowe, S. (2021). Critical digital literacy as a method for teaching tactics of response to online surveillance and privacy erosion. *Computers and composition*. 61, Article 102654. <https://doi.org/10.1016/j.compcom.2021.102654>
- Beigi, G., & Liu, H. (2020). A survey on privacy in social media: Identification, mitigation, and applications. *ACM Transactions on data science*. 1(1), 1–38. <https://doi.org/10.1145/3343038>
- Boateng, R. (2022). Digital inclusion and privacy awareness in sub-Saharan Africa. *Information technology for development*. 28(1), 97–115. <https://doi.org/10.1080/02681102.2021.1942082>
- Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidence: Privacy control frames and disclosure of information. *Social psychological and personality science*. 4(3), 340–347. <https://doi.org/10.1177/1948550612459767>
- Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. SAGE Publications.
- Chen, H. T. (2018). Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American behavioral scientist*. 62(10), 1392–1412. <https://doi.org/10.1177/0002764218787868>
- Christofides, E., Muise, A., & Desmarais, S. (2012). Hey mom, what's on your Facebook? Comparing Facebook use and privacy habits of adolescents and their mothers. *Computers in human behavior*. 28(5), 1983–1991. <https://doi.org/10.1016/j.chb.2012.05.016>
- Ciftci, U. A., Yuksek, G., & Demir, I. (2023). My face my choice: Privacy-enhancing deepfakes for social media anonymization. Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, 1369–1379.
- Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE Publications.
- Custers, B., van der Hof, S., & Schermer, B. (2014). Privacy expectations of social media users:

The role of informed consent in privacy policies. *Policy & internet*. 6(3), 268–295.
<https://doi.org/10.1002/1944-2866.POI365>

Das, S., Dev, J., & Srinivasan, K. (2018). Modularity is the key to a new approach to social media privacy policies. Proceedings of the 7th Mexican Conference on Human-Computer Interaction, 1–4. <https://doi.org/10.1145/3293578.3293582>

Donald, D. A., Srinivas, T. S. S., Rekha, K., Anjali, D., & Srihith, I. D. (2023). The data revolution:
 A comprehensive survey on datafication. *International Journal of advanced research in science, communication and technology*. 3(1), 41–51.

European Parliamentary Research Service. (2019). A governance framework for algorithmic accountability and transparency (PE 624.262). Panel for the Future of Science and Technology. [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU\(2019\)6242_62_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)6242_62_EN.pdf)

Eveleth, L., Stone, R., & Eveleth, D. (2021). Understanding social media users' privacy protection behaviors. *Journal of computer information systems*. 61(4), 342–351.
<https://doi.org/10.1080/08874417.2021.1918320>

Fernandes, T., & Pereira, N. (2021). Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online? *Telematics and informatics*. 65, Article 101717.
<https://doi.org/10.1016/j.tele.2021.101717>

Fosu, M. (2016). A linguistic description of the language of Ghanaian newspapers: Implications for the readability, comprehensibility and information function of the Ghanaian press. *Ghana journal of linguistics*. 5(1), 1–36.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security*. 77, 226–261. <https://doi.org/10.1016/j.cose.2018.04.002>

Hennink, M., & Kaiser, B. N. (2021). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social science & medicine*. 292, Article 114523.
<https://doi.org/10.1016/j.socscimed.2021.114523>

Heravi, A., Mubarak, S., & Choo, K.-K. R. (2018). Information privacy in online social networks:
 Uses and gratification perspective. *Computers in human behavior*. 84, 441–459.
<https://doi.org/10.1016/j.chb.2018.03.012>



- 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, Article 102498. <https://doi.org/10.1016/j.ijhcs.2020.102498>
- Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? *Federal trade commission privacy roundtable*, 1–22.
- Ibdah, D., Lachtar, N., Meenakshi, S., & Bacha, A. (2016). Why should I read the privacy policy? I just need the service: A study on attitudes and perceptions towards privacy policies. *IEEE Access*, 4, 1–10.
- Jain, A., & Sahoo, S. K. (2021). Online social networks security and privacy: Comprehensive review and analysis. *Complex & intelligent systems*. 7(5), 2157–2177. <https://doi.org/10.1007/s40747-021-00401-y>
- Jozani, M., Ayaburi, E., Ko, M., & Choo, K.-K. R. (2020). Privacy concerns and benefits of engagement with social media enabling apps: A privacy calculus perspective. *Computers in Human Behavior*. 107, Article 106260. <https://doi.org/10.1016/j.chb.2020.106260>
- Katz, E., Blumler, J. G., & Gurevitch, M. (1974). Utilization of mass communication by the individual. In J. G. Blumler & E. Katz (Eds.), *The uses of mass communications: Current perspectives on gratifications research*. SAGE Publications, 19–32).
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*. 64, 122–134. <https://doi.org/10.1016/j.cose.2015.07.002>
- 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>
- Krueger, R. A., & Casey, M. A. (2015). *Focus groups: A practical guide for applied research* (5th ed.). SAGE Publications.
- Kuczerawy, A., & Coudert, F. (2011). Privacy settings in social networking sites: Is it fair? Proceedings of the 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust, 1300–1303. <https://doi.org/10.1109/PASSAT/SocialCom.2011.109>
- Kumar, S., Saravanakumar, K., & Deepa, K. (2016). On privacy and security in social media – A

comprehensive study. *Procedia computer science*. 78, 114–119.
<https://doi.org/10.1016/j.procs.2016.02.019>

Latzer, M., & Festic, N. (2019). A guideline for understanding and measuring algorithmic governance in everyday life. *Internet policy review*. 8(2), 1–19.
<https://doi.org/10.14763/2019.2.1415>

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of computer-mediated communication*. 14(1), 79–100. <https://doi.org/10.1111/j.1083-6101.2008.01432.x>

Lie, D., Austin, L. M., Sun, P., & Qiu, W. (2022). Automating accountability? Privacy policies, data transparency, and the third-party problem. *University of Toronto law journal*. 72(2), 155–188. <https://doi.org/10.3138/utlj-2021-0027>

Litt, E. (2013). Knock, knock. Who's there? The imagined audience. *Journal of broadcasting & electronic Media*. 57(3), 330–345. <https://doi.org/10.1080/08838151.2013.816712>

Litt, E., & Hargittai, E. (2014). Smile, snap, and share? A nuanced approach to privacy and online photo-sharing. *Poetics*. 42, 1–21. <https://doi.org/10.1016/j.poetic.2013.10.002>

Markos, E., Peña, P., Labrecque, L. I., & Swani, K. (2023). Are data breaches the new norm? Exploring data breach trends, consumer sentiment, and responses to security invasions. *Journal of consumer affairs*. 57(3), 1089–1119. <https://doi.org/10.1111/joca.12521>

McClain, C., Faverio, M., Anderson, M., & Park, E. (2023). How Americans view data privacy: Tech companies, AI, regulation, passwords, and policies. *Pew Research Center*.
<https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>

Meier, Y., Schäwel, J., & Krämer, N. C. (2020). The shorter the better? Effects of privacy policy length on online privacy decision making. *Media and communication*. 8(2), 291–301.
<https://doi.org/10.17645/mac.v8i2.2847>

Meral, K. Z. (2021). Social media short video sharing TikTok application and ethics: Data privacy and addiction issues. In M. N. Taskiran & F. Pinarbaşı (Eds.), *Multidisciplinary approaches to ethics in the digital era* (pp. 147–165). IGI Global. <https://doi.org/10.4018/978-1-7998-4117-3.ch010>

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs*. 41(1), 100–126.
<https://doi.org/10.1111/j.1745-6606.2006.00070.x>

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy



policies and terms of service policies of social networking services. *Information, communication & society*. 23(1), 128–147. <https://doi.org/10.1080/1369118X.2018.1486870>

Owusu, A., Taana, I. H., Bakare, A. S., Abdurrahman, D. T., & Edem, F. (2020). Investigating the nexus between mobile apps adoption and privacy concerns among users: An empirical analysis from Ghana. *Technium social sciences journal*. 10, 167–181.

Petersen, C., & Lehmann, C. U. (2018). Social media in health care: Time for transparent privacy policies and consent for data use and disclosure. *Applied clinical informatics*. 9(4), 856–859. <https://doi.org/10.1055/s-0038-1675811>

Quan-Haase, A., & Young, A. L. (2014). The uses and gratifications (U&G) approach as a lens for studying social media practice. In R. S. Fortner & P. M. Fackler (Eds.). *The handbook of media and mass communication theory* Wiley-Blackwell, 269–286. <https://doi.org/10.1002/9781118591178.ch15>

Quinn, K. (2016). Why we share: A uses and gratifications approach to privacy regulation in social media use. *Journal of broadcasting & electronic media*. 60(1), 61–86. <https://doi.org/10.1080/08838151.2015.1127245>

Rafique, G. M. (2017). Personal information sharing behaviour of university students via online social networks. *Library philosophy and practice*. Article 1622.

Salleh, N., Hussein, R., Mohamed, N., & Aditiawarman, U. (2013). An empirical study of the factors influencing information disclosure behaviour in social networking sites. 2013 International Conference on Advanced Computer Science Applications and Technologies, 181–185. <https://doi.org/10.1109/ACSAT.2013.43>

Shao, H., Li, X., & Wang, G. (2022). Are you tired? I am: Trying to understand privacy fatigue of social media users. CHI Conference on Human Factors in Computing Systems Extended Abstracts, Article 326, 1–7. <https://doi.org/10.1145/3491101.3519782>

Singh, M. (2021). Privacy preservation techniques for social network users. *2021 International Conference on Computational Methodologies and Communication*, 127–131. <https://doi.org/10.1109/ICCMC51019.2021.9418387>

Smock, A. D., Ellison, N. B., Lampe, C., & Wohn, D. Y. (2011). Facebook as a toolkit: A uses and gratifications approach to unbundling feature use. *Computers in Human Behavior*. 27(6), 2322–2329. <https://doi.org/10.1016/j.chb.2011.07.011>

Stutzman, F., & Hartzog, W. (2012). Boundary regulation in social media. Proceedings of the

ACM 2012. *Conference on computer supported cooperative work*. 769–778.
<https://doi.org/10.1145/2145204.2145320>

Such, J. M., & Rovatsos, M. (2016). Privacy policy negotiation in social media. *ACM transactions on autonomous and adaptive systems*. 11(1), Article 4, 1–29. <https://doi.org/10.1145/2843948>

Susser, D., Roessler, B., & Nissenbaum, H. (2019). Online manipulation: Hidden influences in a digital world. *Georgetown Law Technology Review*. 4(1), 1–45.

Taddicken, M. (2014). The ‘privacy paradox’ in the social web: The impact of privacy concerns, disclosure ratings, and web literacy on social media usage. *Journal of computer mediated communication*. 19(2), 248–273. <https://doi.org/10.1111/jcc4.12052>

Thomas, A., & Gupta, V. (2021). Social capital theory, social exchange theory, social cognitive theory, financial literacy, and the role of knowledge sharing as a moderator in enhancing financial wellbeing. *Frontiers in psychology*. 12, Article 664638.
<https://doi.org/10.3389/fpsyg.2021.664638>

Trifiro, B. M. (2022). Breaking your boundaries: How TikTok use impacts privacy concerns among influencers. *Mass Communication and Society*. 25(6), 820–843.
<https://doi.org/10.1080/15205436.2022.2046031>

Tuunainen, V., Oitkanen, O., & Hovi, M. (2016). Users' awareness of privacy on online social networking sites – Case Facebook. 29th Bled eConference: Digital Economy, 1–10.

Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012). Smart privacy options: How users manage what they share on social networking sites. *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work*. 769–778.
<https://doi.org/10.1145/2145204.2145320>

van Manen, M., & van Manen, M. (2021). Doing phenomenological research and writing. *Qualitative health research*. 31(6), 1069–1082. <https://doi.org/10.1177/10497323211003058>

Vgena, K., Kitsiou, A., & Kalloniatis, C. (2022). Understanding the role of users’ sociolocation attributes and their privacy implications on social media. *Information & computer security*. 30(5), 705–729. <https://doi.org/10.1108/ICS-09-2021-0136>

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International journal of information management*. 36(4), 531–542. <https://doi.org/10.1016/j.ijinfomgt.2016.03.003>

Whiting, A., & Williams, D. (2013). Why people use social media: A uses and gratifications

approach. *Qualitative Market Research: An international journal*. 16(4), 362–369.
[://doi.org/10.1108/QMR-06-2013-0041](https://doi.org/10.1108/QMR-06-2013-0041)

Wisniewski, P. J., Knijnenburg, B. P., & Lipford, H. R. (2017). Making privacy personal: Profiling social network users to inform privacy education and nudging. *International journal of human-computer studies*. 98, 95–108. <https://doi.org/10.1016/j.ijhcs.2016.09.006>

Wu, L., Majedi, M., Ghazinour, K., & Barker, K. (2010). Analysis of social networking privacy policies. *Proceedings of the 2nd international conference on social informatics*, 1–5.

Yang, R., Ng, Y. J., & Vishwanath, A. (2015). Do social media privacy policies matter? Evaluating the effects of familiarity and privacy seals on cognitive processing. *48th international conference on system sciences*. 3463–3472.
<https://doi.org/10.1109/HICSS.2015.417>

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. NY: Public Affairs.

About the Authors

Modestus Fosu is an Associate Professor in Language and Communication Studies at the University of Media, Arts and Communication, Institute of Journalism (UniMAC, IJ) in Accra. He holds a PhD in Media and Communication. His research interests cut across political participation, language and the media, indigenous language media, communication and ethics, and climate change communication.

Martin Thompson Kwadzo Ntem is a PMI certified Project Manager who holds a PhD in Communication from the University of South Africa, a Master of Philosophy in Communication and Media Studies from the University of Education, Winneba, a Master of Arts in Media Management, and a Bachelor of Arts in Communication from the University of Media, Arts and Communication. He is a lecturer at the Institute of Journalism, a constituent of the University of Media, Arts, and Communication in Ghana. His research interests are communication, media representation, framing, and new media.

Wise Kwame Osei is a PhD student at the University of South Africa. He holds a Master's in Global Journalism from the NLA University College, Norway. He also holds a master's in communication and journalism from the Ghana Institute of Journalism, now the University of



Media, Arts and Communication. His research interests include new media systems, artificial intelligence, gender and youth advocacy, journalism, and global media research.