

UNDERSTANDING THE SOCIAL MEDIA BARGAIN: THE IMPACT OF DATA PRIVACY ISSUES AMONG URBAN YOUTH IN BOTSWANA

Mmuso K *

Department of Sociology, Faculty of Social Sciences, University of Botswana, Botswana

Abstract: Social media platforms present themselves as free to users, but they operate by collecting and monetising personal data. This creates a clear tension between digital access and personal privacy. In Botswana, as in many emerging economies, young people use these platforms daily for communication, work and social connection. However, little is known about how they understand the privacy trade-offs they make. This study had three main objectives. Firstly, to examine how urban youth in Botswana negotiate the exchange of their personal data for access to social media. Secondly, to assess whether they are adequately informed about their legal rights regarding data privacy. Thirdly, to identify gaps between Botswana's legal protections and young people's lived experiences of data privacy. The research used a qualitative design. Semi-structured interviews were conducted with 15 urban youth aged 18–30 who actively use social media platforms. A content analysis of Botswana's Data Protection Act (2024) and the Cybercrime and Computer-Related Crimes Act (2018) was also conducted. The findings show three things. Most young participants had a limited understanding of digital privacy. They often equated privacy with hiding their profile or restricting posts to friends. Few knew their rights under Botswana's data protection laws. At the same time, they saw clear benefits to using social media, including social connection and income from online work. Many accepted data sharing as a normal and unavoidable part of using these platforms. The study also found significant gaps in how existing laws are enforced and communicated to the public. This research contributes to the growing literature on data privacy and digital governance in the Global South. It provides empirical evidence from Botswana, a context that has received little attention in this field. The study concludes that legal reform alone is not enough. Effective protection of young people's data requires targeted public education about digital privacy and stronger regulatory enforcement. Without these steps, the social media bargain will remain unbalanced, with users bearing most of the risk.

Keywords: Botswana, data privacy, personal data, social media, public awareness, digital literacy

Introduction

Social media platforms are often perceived as free services; users engage with content without direct financial payments. However, this model masks a critical economic exchange: personal data for platform access. Zuboff (2019) highlights how companies gather and monetize user behaviour, transforming "behavioural surplus" into predictive products for advertisers. This creates an "extraction architecture" that commodifies human experiences. Couldry and Mejias (2019) refer to the appropriation of user data from developing countries as "data colonialism," which exacerbates economic dependencies and power imbalances. For youth in emerging economies, social media is vital for employment, social connections, and information access. Despite the World Bank's (2021) acknowledgment of digital transformation in Africa, young individuals often lack understanding of data privacy risks. This study conceptualises this interaction as the "social media bargain": the exchange of immediate digital engagement for potential data vulnerabilities. While data privacy issues have been widely studied in Western contexts, there is a gap in research regarding how urban youth in Botswana navigate this bargain.

*Corresponding Author's Email: keseego.mmuso@gmail.com



Botswana's internet access is growing, with 68.9% of households connected, primarily via mobile devices (Statistics Botswana, 2025). In response to privacy concerns, the government has enacted data protection laws. However, having legislation does not guarantee protection. Research shows that urban youth are active digital users (Lesitaokana, 2024), yet their awareness of these laws and their enforcement remains unclear. This study addresses two main issues: first, how young people in Botswana negotiate the balance between social media use and data privacy, and second, their understanding of existing legal frameworks. The study aims to: 1) investigate urban youth's perceptions of personal data trade-offs for social media access, 2) evaluate their awareness of rights under the Data Protection Act, and 3) identify gaps between legal protections and user experiences.

Overall, this research contributes empirical data from Botswana, enriching literature on data governance in the Global South, while applying theories of surveillance capitalism and networked privacy. The findings will offer recommendations for policymakers and educators to improve digital literacy and data protection for youth. The article is structured to include background context, a literature review, a theoretical framework, and the methodology.

Background and Context

The rapid digital transformation in Botswana has led to new regulatory measures, notably the Data Protection Act (2024) and the Cybercrime and Computer-Related Crimes Act (2018). The Data Protection Act (2018) originally set out Botswana's legal framework for personal data governance, which was later strengthened through Data Protection Act (2024). The Act governs the processing of personal data, granting individuals rights such as access, correction, deletion, and objection to certain processing practices, including targeted advertising. It imposes compliance responsibilities on both public and private organizations. Meanwhile, the Cybercrime Act penalizes various online offenses, such as unauthorized data access and computer-related fraud. However, enacting laws does not automatically ensure effective protection. Research from other African regions indicates that gaps in implementation, weak enforcement mechanisms and limited public knowledge often weaken even well-crafted legislation. This has been documented even in critical sectors such as digital health (Townsend, 2017). Despite these laws reflecting a commitment to data privacy, effective protection is often hindered by gaps in implementation, weak enforcement, and limited public awareness, especially among young digital users in urban areas.

This analysis focuses on urban youth aged 18 to 30, who are the most active social media users in Botswana. Studies have shown that they are most frequent users of social media among all ages, with mobile phones being routinely and centrally utilized for social interaction (Lesitaokana, 2016; Lesitaokana, 2024). Young individuals may disclose too much personal information, misinterpret privacy settings, or fail to recognize how platforms keep data from temporary posts and stories (Acquisti, Brandimarte & Loewenstein, 2015; Mosweu & Ngoepe, 2019). Given these issues, there is a pressing need for empirical research to understand how urban youth perceive privacy, their awareness of legal protections, and the trade-offs involved in using social media. The following section will review relevant literature and outline the theoretical framework for this study.

Literature Review

Social Media Adoption and Use

Social media platforms have transformed user interactions with digital services, creating a complex economic model where user data acts as currency. Platforms like Facebook, Instagram, TikTok, WhatsApp, and X (formerly Twitter) operate within "surveillance capitalism," a term coined by Zuboff (2019) to describe the collection and monetization of user behaviour data. Users generate data through every click, like, and share, which is then utilized by advertisers to influence consumer behaviour.

Despite awareness of advertising, many users remain unaware of the extent of data collection and the creation of their behavioural profiles.

Researchers like Acquisti, Brandimarte, and Loewenstein (2015) highlight the “privacy paradox,” showing that individuals underestimate the long-term consequences of sharing personal information online. Even those concerned about privacy continue to share data for immediate social or entertainment benefits. Similarly, Mosweu and Ngoepe (2019) found that professional social media users in Botswana often misunderstand how data is kept and shared, believing that deleting posts removes them entirely from servers. Data extractivism, defined by Couldry and Mejias (2019), describes how companies benefit from user-generated content without fair compensation or informed consent. This issue reveals structural power imbalances, particularly in Africa, where data generated locally is leveraged by firms in the U.S. and China without benefits returning to the source nations. The World Bank (2021) warns that African countries may become passive consumers in the global digital economy without proactive measures.

Enforcement gaps further complicate this problem. Townsend (2017) found that while data protection laws are increasingly enacted in several African nations, they often suffer from poor enforcement, lack of regulatory expertise, and compliance issues with multinational firms. Consequently, citizens' data may be legally protected but remains vulnerable in practice.

The Social Media Bargain

The “social media bargain” describes how users, especially young people, engage with digital platforms. It involves an implicit trade-off: users get free access and connectivity while providing personal data that platforms monetize. This relationship is ongoing and characterized by information asymmetry: platforms know much about users, who often lack insight into data use (Zuboff, 2019). For many young people, especially in emerging economies, social media participation is essential for maintaining friendships and accessing jobs, making it difficult to opt out.

Lesitaokana (2016) noted that urban youth in Botswana rely heavily on social media, where being offline can lead to social penalties. This makes the bargain skewed; users are compelled to stay engaged, diminishing their power to demand better privacy practices. Research shows that even when aware of privacy risks, users prioritize immediate rewards over future harms (Acquisti et al., 2015). For example, temporary posts feel low-risk because platforms design them that way, despite data retention. In Botswana, Mosweu and Ngoepe (2019) pointed out that the social media bargain is influenced by limited digital literacy and legal recourse. Users may share sensitive data not out of carelessness, but due to a lack of understanding of privacy implications. Structural factors, such as digital inequality, further limit choices for those with fewer resources. For instance, a young person using Instagram for business cannot easily switch to a more privacy-respecting platform.

Overall, existing literature describes the social media bargain as voluntary in form yet constrained in reality. Users make these exchanges for resources and social connection, but their choices are heavily influenced by social norms, economic necessity, and platform design. To effectively address privacy risks, interventions must focus not just on individual knowledge but also on the broader conditions that make disengagement difficult.

Data Protection Frameworks and Enforcement Realities

Botswana's primary data protection legislation, the Data Protection Act (2024), outlines eight principles aligned with international standards like the GDPR. These include lawful processing, purpose limitation, data minimization, and data subject rights. Individuals can access, correct, or delete their data and file complaints. However, there remains a significant gap between legislation and its practical enforcement, a point highlighted by Townsend (2017) and Mosweu and Ngoepe (2019), who noted

weak enforcement due to underfunded regulators and low public awareness of laws like the Cybercrime and Computer-Related Crimes Act.

Comparative studies show similar challenges in South Africa and Kenya, where awareness of rights and compliance levels are lacking. In South Africa, the Protection of Personal Information Act (POPIA) has been in effect since 2020, yet the Information Regulator has reported persistent compliance issues, including a notable case where the Department of Justice and Constitutional Development was fined R5 million for failing to renew critical security licences (South African Government News Agency, 2023). Despite active public awareness campaigns by the Regulator, awareness of data rights among ordinary citizens remains limited (Bowmans, 2025). Similarly, Kenya's Data Protection Act (2019) has established the Office of the Data Protection Commissioner (ODPC), which has registered over 7,000 data handlers and issued dozens of enforcement notices (ODPC, 2024). However, scholars note that enforcement remains inconsistent, hindered by limited institutional capacity, regulatory fragmentation, and low public awareness (Jumaa & Faturoti, 2025). This indicates that Botswana's enforcement issues are part of a broader regional trend. Despite existing frameworks and the heavy use of social media by young people, few empirical studies explore their awareness of data protection laws and experiences with privacy. This study aims to fill that gap.

Theoretical Framework

This study uses two theoretical perspectives: surveillance capitalism, as developed by Zuboff (2019) and data colonialism, articulated by Couldry and Mejias (2019). Together, they provide the tools to understand how social media platforms extract, commodify and profit from user data, particularly among young people in emerging economies like Botswana.

Surveillance Capitalism

Zuboff's (2019) concept of surveillance capitalism highlights a new economic model emerging in the early twenty-first century, primarily adopted by large tech companies like Google, Facebook (now Meta) and Amazon. Unlike traditional capitalism, which extracts value from labour and resources, surveillance capitalism derives value from human experiences. Zuboff explains that companies collect "behavioural surplus", vast amounts of data from users' online activities such as clicks, searches and social interactions. This data is used to create predictive algorithms that are sold to advertisers and other entities.

He further emphasizes that surveillance capitalism represents not just a business model, but a new form of power. The digital landscape operates as an "extraction architecture" that treats human experiences as free raw materials, with users often unaware of how their data is collected and used. This creates a significant asymmetry between platforms and users regarding knowledge and control over personal data. For this study, the concept provides a framework to understand the conditions under which youth in Botswana engage with social media. These platforms, designed for maximum data extraction, influence users' experiences of connection and identity, with features serving dual functions: user engagement and data generation. While young people may find these features enjoyable, their behaviours ultimately become the products being sold.

Data Colonialism

Couldry and Mejias (2019) build on Zuboff's critique by highlighting global inequalities in data extraction, framing it as a new phase of colonialism where data replaces land and labour. They argue that corporations in the Global North appropriate data from users in the Global South without meaningful consent or fair compensation. This mirrors historical extraction patterns, with behavioural data flowing from peripheral economies to core economies, while costs like privacy loss and surveillance remain local.

This framework is relevant for Botswana and other African nations, where user data is likely stored in countries like South Africa, Europe, or the U.S. Companies like Meta and Google often pay little tax locally compared to the value they extract. Algorithms shaping user experiences are developed elsewhere, reflecting foreign priorities. When data breaches occur, Botswana users face limited legal recourse against multinational platforms that mandate arbitration in foreign jurisdictions.

Data colonialism underscores the power imbalance in the social media exchange. Users in Botswana trade data for access, contributing to a global system that generates profits abroad while creating local risks. Young people often lack awareness of this context, highlighting the need for theoretical exploration.

Integrating the Frameworks for This Study

The study draws on these two frameworks for three key reasons. Surveillance capitalism outlines how platforms extract behavioural data and generate revenue, informing how young people navigate data trade-offs amidst structural forces. Data colonialism highlights the geopolitical aspects of data extraction, revealing why users in Botswana have a different experience in the global data economy compared to those in Europe or North America. This context is crucial for understanding legal awareness and enforcement challenges. These frameworks address the limitations of an individualistic view of privacy. While individual choices around privacy settings and online behaviour are important, surveillance capitalism and data colonialism demonstrate that personal agency is often constrained by unreadable terms of service and the risks of losing access to vital services. Recognizing this structural aspect is essential for effective policy development.

Application to the Botswana Context

Applying these frameworks to Botswana generates specific analytical expectations. From surveillance capitalism, the study expects that social media platforms used by youth in Botswana will exhibit an extractive logic where users' behavioural data is collected, analyzed and monetized, often without their awareness or consent. Privacy settings will likely favour data sharing and even ephemeral features like stories will generate data retained by the platforms.

Regarding data colonialism, the theoretical framework suggests that youth in Botswana will have less awareness of their data rights compared to users in jurisdictions with stronger regulatory frameworks, such as the EU. They will have fewer avenues for exercising those rights and will be largely overlooked in the platforms' governance structures, which primarily cater to wealthier markets. These expectations are not definitive but serve as a framework for interpreting the findings from interviews and document analyses. If young people express concerns about privacy yet continue to share data, surveillance capitalism explains the cost of opting out. Similarly, if they are unaware of the Data Protection Act, data colonialism provides context regarding the impact of weaker enforcement and accountability in the Global South. Thus, the study uses these frameworks as interpretive tools rather than rigid hypotheses. The findings section will detail participants' insights and document analysis, while the discussion will revisit surveillance capitalism and data colonialism to explore how data extraction operates in Botswana and examine the limitations of current legal protections.

Methodology

Research Design and Approach

This study utilized a qualitative exploratory research design to investigate the data privacy practices and perceptions of urban youth in Botswana. While quantitative surveys could measure how many young people adjust privacy settings, qualitative methods offer deeper insights into why they make specific choices and how they perceive privacy. This study focuses on understanding participants' subjective experiences regarding their online activities and privacy practices. The research questions

aim to explore processes and meanings rather than frequencies. Specifically, they inquire how young people negotiate data trade-offs and whether they are informed about their rights, prioritizing depth over breadth through rich data from a smaller participant group.

Data Collection

Data were collected through semi-structured interviews and content analysis of legal documents. This combination enabled cross-referencing participants' awareness of data protection laws with the legislation itself.

Semi-structured interviews: involved 15 urban youth aged 18 to 30. This flexible format allowed for the exploration of key topics like social media use and experiences with privacy-related incidents. Interviews were conducted in person or via secure online platforms and lasted 35 to 65 minutes, with audio recordings transcribed verbatim.

Content analysis: focused on Botswana's Data Protection Act (2024), the Cybercrime and Computer-Related Crimes Act (2018), and various privacy policies from major social media platforms. This analysis aimed to identify formal legal protections and user rights, which served as a basis for comparing participant awareness.

Study Participants and Sampling

Participants were selected through purposive sampling, focusing on those aged 18-30, living in urban Botswana, and active on social media daily. No exclusions were made based on gender, education, or socio-economic status, though a diverse representation was sought. Recruitment strategies included university networks, community boards, and social media, supplemented by snowball sampling. The final sample comprised 15 participants (eight women and seven men) aged 19 to 29, with varied educational and employment backgrounds, chosen based on data saturation.

Table 1: Participant Demographics

Pseudonym	Age	Gender	Location	Occupation
Participant 1	19	Male	Gaborone	Student
Participant 2	23	Male	Gaborone	Unemployed
Participant 3	22	Female	Gaborone	Student
Participant 4	26	Female	Francistown	Employed
Participant 5	20	Female	Francistown	Student
Participant 6	24	Female	Selibe-Phikwe	Self-employed
Participant 7	24	Male	Francistown	Employed
Participant 8	29	Male	Gaborone	Freelance
Participant 9	26	Male	Lobatse	Employed
Participant 10	22	Male	Gaborone	Student
Participant 11	21	Female	Gaborone	Student
Participant 12	27	Female	Gaborone	Self-employed
Participant 13	30	Male	Gaborone	Employed
Participant 14	28	Female	Gaborone	Employed
Participant 15	23	Female	Gaborone	Unemployed

Findings

The analysis of interview data and legal documents revealed four key themes regarding urban youth in Botswana and their social media use and personal data privacy: (1) understanding of privacy, (2) perceived benefits of "free" social media, (3) privacy risks experienced, and (4) gaps in legal awareness and enforcement. These themes are supported by participant quotes (using pseudonyms) and relevant document analysis.

Conceptual Understanding of Privacy Among Youth

Interviews indicated that most participants had a limited and often inaccurate understanding of digital privacy, primarily equating it with visibility control. Responses like "keeping my profile hidden from people I don't know" (Participant 3, 22, Gaborone) and "only my friends can see what I post" (Participant 7, 24, Francistown) were common. Few mentioned data collection, algorithmic tracking, or third-party access. Misconceptions about social media data handling were also prevalent. One participant believed that disappearing Instagram stories didn't remain on the platform: "If it disappears after 24 hours, I assume it's gone." (Participant 11, 21, Gaborone). Another was surprised to learn that deleted WhatsApp messages might still be retained: "I never thought about whether they stay on WhatsApp's servers." (Participant 9, 26, Lobatse). Such misunderstandings demonstrate a gap between user assumptions and actual data practices. As Mosweu and Ngoepe (2019) observed in their study of Botswana public sector workers, the perception that deleting content removes it completely is widespread but incorrect. Platform privacy policies typically disclose that data may be retained for extended periods, but participants in this study had rarely read these policies. When asked directly, only two of the fifteen participants reported having ever read a social media platform's privacy policy from beginning to end.

Awareness of Botswana's Data Protection Act (2024) and the Cybercrime Act (2018) was notably low; no participant could name either law. Even when prompted, most had no recollection of them. One remarked: "I just assume if something bad happens, I can report it to the police." (Participant 14, 28, Gaborone). This lack of awareness prevents participants from exercising their rights, such as access and deletion. Participants generally normalized data collection as a fact of life, with many expressing resignation: "I know my data is out there...but I still use the apps." (Participant 2, 23, Gaborone). This sense of inevitability regarding privacy loss suggests that even when aware of data collection, participants see no meaningful alternatives.

The Perceived Benefits of "Free" Social Media

Participants identified significant benefits of social media use, categorized into social connectivity, economic opportunity and identity performance.

Social Connectivity was the most mentioned benefit. Participants highlighted social media as vital for maintaining friendships, especially with distant peers. One participant noted, "Without Instagram, I would never talk to my friends in South Africa, the UK, or Australia." (Participant 5, female, 20, Francistown). Instant communication and sharing experiences were seen as invaluable compared to older, more expensive forms of communication.

Economic Opportunity was another key benefit, particularly for those freelancing or seeking jobs. Many used social media to generate income. A participant selling handmade jewelry shared, "I post my work on Instagram; that's where my customers find me. Without it, I'd need to rent a shop, so I can't complain about sharing my information." (Participant 12, female, 27, Gaborone). A freelance graphic designer noted the importance of being visible on social platforms to attract clients, "If you are a creative person in Botswana, you have to be on social media. That is where the jobs are. Clients message me on WhatsApp, they see my work on Instagram. I tried using a website once, but no one visited it. People want to see you on the platforms they already use." (Participant 8, male, 29, Gaborone)

These statements illustrate the structural dependency described in the theoretical framework. Participants do not choose to use specific platforms because they trust them or value their privacy features. They use them because their customers, employers, and professional networks are already there. This dependency fundamentally shapes the social media bargain: opting out is not a realistic option for those who rely on these platforms for income.

Identity Performance was the third benefit. Participants described how social media allowed them to curate online personas reflecting their aspirations and values. One participant expressed, "Social media lets me be who I want to be. In real life, people know me as quiet. Online, I can share my art, my opinions, my style. It feels more like me than real life sometimes." (Participant 6, female, 24, Selibe-Phikwe). However, this identity work often required extensive disclosure of personal information. Participants who curated detailed online profiles including photos, location check-ins, relationship status, employment history and personal interests were simultaneously generating the behavioural data that platforms monetize. Few participants recognized this trade-off explicitly. When it was raised during interviews, most responded with versions of "that's just how social media works" (Participant 10, male, 22, Gaborone), indicating that the bargain had become so normalized as to be invisible.

Privacy Risks and Vulnerabilities

Participants reported significant exposure to privacy risks on social media, categorized into four sub-themes: oversharing, digital scams, algorithmic profiling and data breach concerns.

Oversharing was common, with participants sharing personal information to enhance engagement, although opinions on its significance varied. Social pressure played a role, with many feeling compelled to post regularly to avoid being seen as secretive or antisocial. "Sometimes I post things I shouldn't. Like where I am, who I am with, what I am doing. I don't think about it at the time. I just want people to see my life, to comment, to like. Later I might delete it, but by then, who has already seen it?" (Participant 1, male, 19, Gaborone). Social pressure was a significant driver of oversharing. Several participants noted that friends expected them to post regularly, to share updates, and to engage with content. Not posting carried social penalties, including being perceived as secretive, antisocial, or "having something to hide" (Participant 4, female, 26, Francistown). This finding aligns with networked privacy theory (boyd & Marwick, 2011), which argues that privacy is not merely an individual decision but is negotiated within social relationships.

Digital scams were frequently mentioned, with participants recounting experiences with phishing attempts and fraudulent services. One participant recalled almost providing personal information in response to a suspicious message, highlighting the risks of insufficient digital literacy; "Someone messaged me on WhatsApp saying they were from the bank and needed my PIN to verify my account. I almost gave it. But then I thought, why would the bank contact me on WhatsApp? So I called the bank directly and they said it was a scam." (Participant 13, male, 30, Gaborone)

Algorithmic profiling caused unease, as some participants felt monitored after seeing targeted ads for products they had only discussed. Despite platform assurances that microphones aren't used for tracking, this phenomenon contributed to feelings of surveillance. One participant recounted: "I was talking to my friend about wanting to buy new running shoes. We never searched for it online. The next day, my Instagram was full of ads for running shoes. How does that happen? It feels like my phone is listening." (Participant 10, male, 22, Gaborone) While platform policies typically deny that phones actively listen through microphones for advertising purposes, the experience of eerily relevant ads is common and contributes to a sense of surveillance. Participants who noticed this phenomenon expressed discomfort but did not know how to prevent it. Few were aware that they could limit ad tracking through privacy settings.

Data breaches were acknowledged as serious risks, with concerns about who could access shared content. Participants worried about the privacy of their personal information but felt uncertain about

how to protect it or where to find information on data usage. One participant stated: "I don't put anything really private on social media. No banking details, no ID numbers. But photos of my family, my location, my conversations – that stuff is on there. I don't know who can see it or what they do with it. That bothers me, but I don't know what to do about it." (Participant 15, female, 23, Gaborone).

Table 2: Summary of Privacy Risks

Risk Category	Description	Participant Response
Oversharing	Posting locations, relationships, daily routines	"Sometimes I post things I shouldn't" (P1, male, 19)
Digital scams	Phishing messages, fake job offers, fraudulent stores	"Someone messaged me saying they were from the bank" (P13, male, 30)
Algorithmic profiling	Targeted ads based on offline conversations	"It feels like my phone is listening" (P10, male, 22)
Data breaches	Third-party access to personal content	"I don't know who can see it or what they do with it" (P15, female, 23)

Gaps in Legislation Awareness and Regulatory Enforcement

The final theme highlights the disconnect between Botswana's legal framework and participants' awareness of it. Awareness of the Data Protection Act and Cybercrime Act was nearly nonexistent among participants, leading to an inability to exercise their legal rights, such as requesting data deletion or lodging complaints. While the Data Protection Act (2024) establishes comprehensive data subject rights and organizational obligations, implementation provisions are lacking. The Act does not define timelines for addressing complaints or impose significant penalties on non-compliant platform companies. Notably, there is no evidence that the Data Protection Commissioner has actively monitored or enforced regulations against social media platforms in Botswana, indicating an under-resourced regulatory authority.

Participants sensed this enforcement gap, with many expressing doubt that reporting privacy violations would lead to any meaningful action. A common sentiment was, "Even if there is a law, what will happen? The platforms are huge, international. The Botswana government cannot control Facebook. So why would Facebook care what our law says?" (Participant 8, male, 29, Gaborone). This reflects a broader reality that local laws struggle to regulate global platforms due to differing legal standards and the dominance of large technology companies. This perception of power inequalities that local laws cannot constrain global platforms – is grounded in reality. Participants are correct that enforcement against multinational technology companies is difficult and rare. The data colonialism framework (Couldry & Mejias, 2019) explains why: platforms are headquartered in jurisdictions with different legal standards, their terms of service typically mandate dispute resolution in foreign courts, and they face little local accountability in small markets like Botswana.

The findings suggest that regulatory frameworks alone are inadequate. Without public education on data rights, active enforcement and mechanisms to hold international platforms accountable, young people in Botswana will continue to face privacy risks despite existing legislation. The final section of the article discusses the implications of these findings for policy and practice.

Discussion

This study reveals how urban youth in Botswana navigate social media, privacy and the implicit trade-offs of the social media bargain. Drawing on the theoretical frameworks of surveillance capitalism (Zuboff, 2019) and data colonialism (Couldry & Mejias, 2019), along with networked privacy theory (Boyd & Marwick, 2011), the findings underscore the structural and economic forces influencing youth behaviour online. Four key themes emerge: limited privacy understanding, perceived benefits, experienced risks and legal gaps, each with significant implications for policy and future research.

The Social Media Bargain as a Structural Constraint

Participants showed limited awareness of digital privacy yet continued using social media, suggesting a complex "privacy paradox" as documented by Acquisti, Brandimarte and Loewenstein (2015). They were not simply irrational; rather, they faced a lack of alternatives. Many depended on platforms for social connection or economic activity, illustrating that the bargain is non-negotiable. As social media becomes integral to daily life, leaving these platforms means sacrificing vital networks. Surveillance capitalism (Zuboff, 2019) explains this structure: platforms prioritize data extraction over user awareness. The "free" model is a strategy, leaving users with little choice but to engage in the data economy. Effective digital privacy interventions must go beyond individual behaviour change, addressing the structural conditions enforcing platform dependency.

Networked Privacy and Social Pressure

Social pressure significantly influences individuals' sharing practices, aligning with networked privacy theory proposed by Boyd and Marwick (2011). Their research on American teenagers revealed that privacy is less about individual control and more about social negotiation within peer groups. Participants in this study noted expectations from friends to post frequently and engage with content, where not participating could lead to being viewed as secretive or antisocial.

This insight challenges interventions that frame privacy as solely an individual responsibility, suggesting that advising someone to "post less" overlooks the social context of their decisions. Effective interventions should aim to shift group norms, possibly through peer discussions on appropriate sharing or campaigns promoting boundary-setting among friends. Additionally, the networked privacy perspective clarifies why individuals continue to share personal information despite negative outcomes like scams. Leaving these social networks incurs significant practical and social costs, risking exclusion from conversations and experiences. Therefore, interventions must consider these social dynamics to effectively change behaviours.

The Economic Dimension of the Social Media Bargain

Participants in this study highlighted their reliance on social media for economic activities, such as selling products or freelancing. For many, social media is essential for economic survival, not just social connection. While Zuboff (2019) critiques how platforms profit from user data, less attention has been given to how users generate income through these platforms. For young people in emerging economies with high unemployment, social media serves as vital economic infrastructure, providing access to markets and customers.

This economic dependency shifts the power dynamics of social media use. Users relying on apps like Instagram for income face challenges when considering alternatives due to the risk of losing their livelihood. Platforms exploit this dependency, often lacking incentives to enhance privacy protections. From a policy standpoint, addressing data protection issues must align with broader economic strategies. While improving digital literacy and data laws is important, it is not enough if users remain reliant on platforms that commodify their data. Developing alternative digital infrastructures, such as

cooperative-owned or public interest networks, could offer real choices, although these initiatives face obstacles like funding and technical challenges.

Gaps Between Law and Practice

The awareness of Botswana's Data Protection Act and Cybercrime Act is alarmingly low among participants, with skepticism about enforcement mirroring findings across Africa. Townsend (2017) and Mosweu and Ngoepe (2019) noted similar issues, highlighting that while laws exist, public knowledge is scarce and enforcement is weak. The data colonialism framework (Couldry & Mejias, 2019) illustrates this persistent gap. Botswana's legal frameworks assume that data processing occurs within specific jurisdictional boundaries, but social media platforms operate globally, creating complications in enforcement when data crosses borders. As one participant noted, "The Botswana government cannot control Facebook. So why would Facebook care what our law says?" This is a realistic assessment of the situation.

To address these issues, Botswana must seek regional or international cooperation. Strengthening the Data Protection Commissioner's office and enhancing public awareness are valuable steps, but they will have limited impact without collaborative efforts with other Southern African Development Community (SADC) countries to establish common data protection standards and joint enforcement mechanisms.

Limitations of the Study

This study has several limitations. Firstly, the sample consisted of only 15 urban participants in Botswana, limiting the generalizability of findings to rural youth, older populations, or other areas. Secondly, reliance on self-reported data may lead to misrepresentation of privacy practices, either consciously or unconsciously. Thirdly, while the interviews captured participants' perceptions, they did not reflect actual online behaviours, which may differ. Fourth, the absence of platform data analysis missed the opportunity for a more objective view of data sharing practices. Lastly, the research was conducted at a single point in time, making the findings susceptible to rapid changes in the digital landscape.

Suggestions for Future Research

The findings indicate several avenues for future research. To begin with, a larger quantitative study could assess the prevalence of urban youth in Botswana who understand data protection rights, have experienced privacy violations and identify demographic predictors of awareness. In addition, comparative research across African countries like Kenya, Nigeria, and South Africa could reveal regional differences in privacy awareness and legal impacts. Moreover, ethnographic studies could document actual online behaviours, such as privacy settings management and responses to data requests. Fourth, examining the economic dependency of young people on platform-mediated income could highlight how it affects their privacy trade-offs. Finally, evaluation research could explore the effectiveness of public awareness campaigns and regulatory enforcement on improving knowledge and platform behaviour. These areas warrant longitudinal, intervention-focused research designs.

Implications for Policy and Practice

This study highlights key implications for policy and practice. Public education on data privacy should target specific misconceptions, such as the belief that disappearing content is permanently deleted. Materials need to be developed in local languages, using channels popular among youth, and assessed for effectiveness. The Data Protection Commissioner's office requires sufficient resources for enforcement, as legislation alone is not enough. This includes staffing, technical expertise, and the authority to investigate and penalize violations.

Botswana should seek regional and international cooperation on data protection, leveraging platforms such as the SADC for harmonized standards and creating bilateral agreements with countries hosting major technology companies. Economic policy must recognize the platform economy's impact on young people's livelihoods. Solutions could involve supporting platform cooperatives and developing portable data rights. Interventions should focus on changing social norms around data sharing through peer-led programs and school curricula, rather than merely providing information.

Conclusion

This study explored how urban youth in Botswana manage social media use and personal data privacy. Findings reveal that while young people benefit from social media for connection, economic opportunities, and identity expression, they operate within a system that disadvantages them. Many participants lacked understanding of digital privacy, misconceptions about data handling, and were unaware of their rights under Botswana's Data Protection and Cybercrime Acts. It also offers three key insights: it provides evidence that surveillance capitalism and data colonialism affect Botswana; the privacy paradox is more about structural constraints than individual choices, as young people find it hard to leave platforms; third, there are significant gaps between awareness and the legal framework.

The social media bargain is inequitable, with platforms profiting from users in the Global South. Addressing this requires more than improving digital literacy. Policymakers need to empower the Data Protection Commissioner, educators must rectify misconceptions (such as the notion that disappearing content is deleted), and regional cooperation in SADC is essential to hold global platforms accountable. Ultimately, Botswana must build digital infrastructures that cater to local needs, or its youth will remain vulnerable, paying the price for "free" services without understanding what they sacrifice.

References

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science (New York, N.Y.)*, 347(6221), 509–514. <https://doi.org/10.1126/science.aaa1465>
- Bowmans. (2025). *Public awareness of data protection and privacy is on the rise in Africa*. BusinessGhana.
- Boyd, d., & Marwick, A. E. (2011, September). Social privacy in networked publics: Teens' attitudes, practices, and strategies. In *A decade in internet time: Symposium on the dynamics of the internet and society*.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2), 77-101.
- Couldry, N., & Mejias, U. A. (2019). *The costs of connection: how data is colonizing human life and appropriating it for capitalism*. Stanford University Press. <https://ebookcentral.proquest.com/lib/kcl/detail.action?docID=5789180>
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches (4th ed.)*. SAGE Publications.
- Data Protection Act, 2024. *Government of Botswana*. Government Printer.
- Data Protection Act, 2018. *Government of Botswana*. Government Printer.
- Jumaa, I., & Faturoti, B. (2025). Enforcing data privacy in Kenya and Nigeria: towards an African approach to regulatory practice. *International Review of Law, Computers & Technology*, 1-26.
- Lesitaokana, W. O. (2016). Urban youth in Botswana and their habitual practice of texting. *GSTF Journal on Media & Communications (JMC)*, 3(1), 6.
- Lesitaokana, W. O. (2024). The Nexus Between Youth and Mobile Phones in Botswana. In *Handbook of Children and Youth Studies* (pp. 829-841). Singapore: Springer Nature Singapore.
- Mosweu, T., & Ngoepe, M. (2019). 'Here one moment, gone the next': A framework for liquid communication generated through social media platforms in the Botswana public sector. *South African Journal of Information Management*, 21(1), 1-11.
- Office of the Data Protection Commissioner. (2024). Kenya marks 5 years since the implementation of the Data Protection Act. *Government of Kenya*.
- South African Government News Agency. (2023, July 4). *Information Regulator fines Justice Department*. SAnews.gov.za. <https://www.sanews.gov.za/south-africa/information-regulator-fines-justice-department>

Statistics Botswana. (2025). Information and Communication Technology (ICT) Statistics Report 2024. *Statistics Botswana*.

Townsend, B. A. (2017). Privacy and data protection in eHealth in Africa. *PhD diss., University of Cape Town*.

World Bank. (2021). Digital Africa: Technological transformation for jobs. World Bank Group. <https://openknowledge.worldbank.org/handle/10986/35014>

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. *Journal of Information Ethics*, 33(1), 84-85.