Qualitative Pilot Study Report

A Pilot Study Exploring How Social Media Users Reconcile Risks with Continued Platform Use

Course: Converting Research into Practice
Course Code: LCDB7010
Course Leader: Dr. Caroline Jawad
Submitted by: Marvin Malthus Gomes
Student ID: 2507129

Submission Date: May 31, 2026

Table of Contents

Part A: Executive Summary 3

Choice of Journal with Metrics 3

Justification of Choice 3

Part B: Article Text 5

Title 5

Abstract 5

Introduction: Research Background and Gap 5

Research Aim, Objectives and Questions 6

Literature Review: Conceptual Territory and Context 7

Privacy Calculus Theory: Explaining Risk-Benefit Evaluation 7
The Privacy Paradox and Digital Resignation 8
Contextual Integrity, Boundary Management and Privacy Practices 8
Social Media as Social, Professional and Moral Infrastructure 9
Wellbeing, Social Comparison and Time Displacement 10
Algorithmic Datafication, Targeted Advertising and AI-Driven Personalisation 10
Misinformation, Trust and Information Integrity 11
Research Gap and Contribution 11
Synthesis of the Literature for the Present Study 12

Methodology 13

Research Approval 13
Research Approach 14
Research Design 14
Participant Selection and Recruitment 15
Data Collection Procedures 15
Data Analysis 16
Quality and Rigour 17
Reflexivity and Pilot Limitations 17
Data Management and Audit Trail 18
Methodological Learning from the Pilot 18

Findings: Emergent Data Observations and Deductions 18

Theme 1: Social media functions as social, professional, communicative and moral infrastructure 19
Theme 2: Risk becomes meaningful when it is concrete, visible or emotionally close 19
Theme 3: Reconciliation is a relational, emotional and practical privacy calculus 20
Theme 4: Protective practices create partial, sometimes symbolic, control 20
Theme 5: Risk awareness usually produces cautious adaptation rather than full withdrawal 21
Theme 6: Ethical comfort requires platform and regulatory responsibility as well as individual mindfulness 21
Cross-Theme Deduction 22
Cross-Participant Data Matrix 22
Thematic Map 23

Conclusion: Contributions, Limitations and Recommendations **24**
Contributions 24
Limitations 25
Recommendations 25
Part C: Reflection on Personal Learning and Skill Development ***26***
Appendices ***28***
Appendix A: Raw Interview Transcript **28**
Appendix B: Coded Transcript **31**
Appendix C: Interview Question Matrix Summary **34**
Appendix D: Cross-Case Theme Development Audit Trail **35**
References ***36***

Part A: Executive Summary

This pilot study examines how six adults who engage with social media find themselves making sense of a range of risks concerning privacy, data, wellbeing, and ethics alongside continuing to use social media platforms. It is interpretivist in nature and employs a qualitative methodology through semi-structured interviews and reflexive thematic analysis in line with that conducted by Braun & Clarke. The new analysis process is now grounded in the six participant-level audit trail documents for P01-P06, which include familiarization notes, master coding list, code to category development, provisional groups, provisional definition and one participant-level write-up. In all six cases examined, the individuals continued engaging with social media not because they remained ignorant of risks. Rather, there was a variety of reasons for continuing usage related to various types of infrastructure social media provided: social media was used by P01 for political voice and consciousness-raising; P02 experienced the social costs of being out of the real-time loop; P03 used Facebook/Messenger for communication and education; P04 uses Facebook and Instagram for sustaining distant relationships; P05 engaged in low exposure intentional use; and P06 used WhatsApp, Messenger, and LinkedIn for communicating. Findings are presented at the end of the report using cross-case analysis, which gives us general themes about the research instead of focusing on individual participants. From this report, we can see that risk only gains significance when it is tangible and emotional; protective mechanisms offer a form of control but not much; continued use is based on adaptive behaviour; and ethical comfort depends on transparency in the platform, stricter regulations, and ethical behaviour on the part of users.

Choice of Journal with Metrics

Journal name and metrics:

Computers in Human Behavior

Publisher: Elsevier

ISSN: 0747-5632

Publication frequency: 12 issues per year

Journal scope: Human Behaviour, Digital Media, Technology Use, Psychology and Human-Computer Interaction

Justification of Choice

"Computers in Human Behavior" is a suitable journal as the research pilot focuses on how users resolve the dilemma of being aware of risks associated with social media usage and continue using these platforms. The research involves human behaviour, privacy calculation, wellbeing,

ethics, and platform responsibility. The qualitative interpretivist method allows for acquiring empiric insights into how regular people cope with the issues mentioned above. The audience of the selected journal may be interested in this research as it touches upon digital behaviour and technology use.

Part B: Article Text

Title

A Pilot Study Exploring How Social Media Users Reconcile Risks with Continued Platform Use

Abstract

This qualitative pilot study explores how social media users reconcile awareness of privacy, data, wellbeing and ethical risks with continued platform use. The study consisted of six participants in semi-structured interviews, followed by a post-interview question on platform, regulatory and individual change. Reflexive thematic analysis, as proposed by Braun and Clarke was used for the data analysis process. The current revised analysis relies on six participant level audit trail documents, which includes familiarisation notes, consolidation master codes, code to category formation, initial code and theme generation. The findings show that the continuation of platform use cannot be justified by a lack of awareness regarding the risks involved. Platforms serve as a social, professional, communicative, informational and ethical structure for users. Privacy dilemma management takes place in terms of selective exposure, selective disclosure, privacy settings, technical protection, minimised use, platform switching, and rationalization through right use, balancing benefits against risks, and being inherently socially embedded. Another critical aspect raised by the analysis relates to the drawbacks of self-regulation by individuals in relation to privacy practices.

Introduction: Research Background and Gap

Social media platforms are now integral parts of the way people live their lives, interact at work, learn at educational institutions, stay in touch with family members, engage in politics, and construct their identities. The use of social media sites like Facebook, Instagram, X/Twitter, WhatsApp, Messenger, LinkedIn, TikTok, and YouTube is now necessary for staying in touch with loved ones, staying informed about current affairs, pursuing educational opportunities, networking, voicing one's opinions, and engaging socially. On the other hand, using social media platforms comes with certain ethical and pragmatic dangers. For instance, individuals can be exposed to privacy concerns, data harvesting, targeted advertising, online fraud, hacking, identity theft, cyber-bullying, doxxing, disinformation, social comparison, loss of time, and pressure regarding wellbeing. The above risks tend to be amplified by the nature of social media platforms, which are designed to encourage engagement, visibility, and data collection. The research background is the well-established gap between privacy attitudes and privacy behaviour. The privacy calculus and privacy paradox literature demonstrate that one

could be concerned with their privacy but continue using digital platforms and providing their personal information (Dinev and Hart, 2006; Norberg, Horne and Horne, 2007; Dienlin, Masur and Trepte, 2023). At the same time, it would be a mistake to view such a gap as irrational user behaviour. Social pressure, convenience, peer visibility, dependency, design defaults, digital literacy, trust, and lack of alternatives impact user decisions as well.

The current pilot study aims to investigate the phenomenon by analysing how individuals make sense of contradictions. Instead of addressing the question of whether continued usage is objectively wrong or right, it is essential to understand why people engage with certain apps in the context of existing risks and possible consequences. One must identify which dangers matter to a user and why they find some benefit in continued engagement with a digital platform despite all the potential harms involved. Practical significance is equally obvious. As individuals use platforms more for social, professional, and informational needs, the sole approach of individual education will not be sufficient. Issues of design, privacy defaults, algorithms, regulation, and digital literacy all come into play as solutions to the issue. In this respect, the paper contributes to academic discussions on privacy calculus and privacy paradox while also generating knowledge for practical use.

The research gap exists for both theoretical and practical purposes. While previous studies have provided some explanation about patterns and consequences of concern, disclosure and well-being, there is little room left for the voices of people themselves in terms of their rationalisation of compromising their well-being and how they deal with the conflict. This approach can be considered most fitting within the context of the LCDB7010 module since it translates a live issue of digital business into practice. Thus, the proposed research considers continued use as a kind of negotiation process in place of a failure of behavioural compliance. The key question here is about staying engaged while protecting one's privacy and well-being.

Research Aim, Objectives and Questions

Using a qualitative interpretivist approach, this pilot study seeks to explore the phenomenon of adults' reconciling between their awareness of the risks involved with their ongoing use of social media sites. This study will not seek to quantify the risk or to test the cause-and-effect relationship. It will concentrate on sensemaking, in other words, the ways participants perceive risks, give reasons for their behaviour and find solutions to mitigate risk and make the platform usage safe and ethical.

The research objectives are:

- To identify the social media platforms and everyday contexts in which users encounter privacy, wellbeing and ethical concerns.
- To examine how users perceive and interpret situations of tension between their awareness of risk and their continued use of social media.
- To explore the techniques, protective practices and rationalisations users employ to manage or explain continued platform use despite awareness of risks.

The research questions are:

1. In which social media platforms and everyday contexts do users most regularly sense tension between their awareness of potential risks and their continued engagement?
2. How do users perceive and interpret periods of tension between privacy concerns, personal wellbeing and continued usage of social media platforms?
3. What techniques or rationalisations do people employ to manage or explain their continuous usage of social media despite being aware of the risks?

Ten semi-structured questions were developed from the above research questions. Questions 1 to 3 related to platform usage and risk awareness, while Questions 4 to 7 related to tension, weighing benefits and risks and their rationalization, and Questions 8 to 10 related to protection and changes in behaviour. Q11 addendum views on what needs to be changed at the platform level, regulator level, and individual level. The alignment between aim, objectives, and research questions is important since this study is qualitative in nature. As such, the intent is not to demonstrate that something is true based on certain assumptions, but to develop a credible explanation for how users navigate contradictory demands in their daily interactions on online platforms.

Literature Review: Conceptual Territory and Context

Privacy Calculus Theory: Explaining Risk-Benefit Evaluation

The Privacy Calculus Theory forms the major sensitizing concept for this pilot study. This theory posits that people decide whether to disclose and use certain platforms based on the balance between the perceived benefits and risks related to their privacy (Dinev and Hart, 2006; Xu et al., 2011). For social media, the benefits might include communication, presentation, social capital, entertainment, news provision, and learning or career opportunities. Risks would include unwarranted disclosure, misuse of data, loss of reputation, monitoring, hacking, or lack

of control over personal data. This theoretical perspective is relevant as participants used cost-benefit language when referring to social media experiences.

Empirical research from recent years indicates that the notion of privacy calculus cannot be regarded as a simple act of rational deliberation. In this case, Nguyen, Tran, and Hoang (2024) indicate that peer privacy risks can impact active and passive use of social networking site in different ways, implying that not only platform-related privacy risks should be considered. Meier and Krämer (2024) further argue that privacy decisions operate at both between-person and within-person levels. In this context, it is necessary to note that the participants have talked about changes occurring over time and involving tightening settings after some problems, switching to other platforms, etc. For this report, Privacy Calculus Theory is consequently used as an interpretive lens in place of a hypothesis-testing model. The theory can provide insight into the idea of trade-offs but does not sufficiently address social, emotional, and ethical conditions under which people continue using platforms despite risks.

The Privacy Paradox and Digital Resignation

The term Privacy Paradox describes the discrepancy between the users' privacy-related concerns and their actual privacy disclosure or use of platforms (Norberg, Horne & Horne, 2007; Dienlin & Trepte, 2015). While earlier studies considered such a phenomenon an illustration of inconsistencies, the results obtained in later studies prove otherwise. As stated by Dienlin, Masur, and Trepte (2023), this paradox cannot be viewed as stable or universal; the user privacy concerns and behaviours may vary depending on different circumstances. This study also proves that the risks associated with the use of social media have been addressed by the participants; they modified their behaviour in a partial manner.

Digital resignation is also able to account for user persistence amid discomfort. Some of the respondents believed that it was too big to avoid the platform systems, while others argued that the terms and conditions do not always make explicit what information is being gathered from the participant. P02 uses the imagery of security as being a closed door that still has windows, whereas P04 perceives the platforms' privacy policies as creating a choice of either accepting them or not using them.

Contextual Integrity, Boundary Management and Privacy Practices

The idea of contextual integrity from Nissenbaum (2010) clarifies the meaning of privacy since it involves information flow within the relevant social context (Nissenbaum, 2010). The phenomenon of social media causes context collapse where the family, friends, co-workers,

employer, strangers, and platforms can become one audience. Studies demonstrate how users try to cope with boundaries through limiting audiences, self-disclosures, privacy settings, and self-censorship (Vitak, 2012; Young and Quan-Haase, 2013; De Wolf et al., 2014; Hargittai and Marwick, 2016). The literature above directly relates to the participant practices. The former applies to P01 and her anonymity tactics; the latter applies to P02 and the hiding of the personal data. Meanwhile, P03 relies on the use of generic location tags and audience filters. P04 refrains from live posts and political/religious discussions. P05 avoids risk through non-disclosure; P06 hides content from everyone except known contacts. Thus, boundary work facilitates the further use of apps. Nonetheless, boundary management is incomplete, since data collection, advertisement systems, and algorithmic reasoning occur outside users' field of perception and control. The emergence of new social media platforms exacerbates the problem. According to Lu et al. (2025), organizational privacy and peer-related issues affect disclosure within short-form videos. Lyianaarachchi et al. (2024) introduce the idea of the multi-privacy paradox and apply it to the phenomenon of virtual influencers.

Social Media as Social, Professional and Moral Infrastructure

Uses and gratifications research helps explain why users remain on social media despite risk. Users continue Uses and Gratifications theory helps to understand why people stay on social media despite the danger. They continue using platforms since they fulfil users' needs of communication, getting information, being entertained, developing relationships and expressing one's identity (Joinson, 2008; Quan-Haase and Young, 2010; Whiting and Williams, 2013). Additionally, social capital theory suggests that the use of platforms might be helpful for building weak ties, bonding and bridging relationships (Ellison, Steinfield, and Lampe, 2007; Ellison et al., 2014; Burke and Kraut, 2016).

Pilot data demonstrates some similarities with previous studies. Thus, P02 explained the need for social media through staying up to date. At the same time, P04 saw its usage as something that would help maintain relationships in foreign countries. In turn, P05 explained the use of Facebook and LinkedIn to connect and get professional information, while P06 regarded WhatsApp, Messenger, and LinkedIn as means for communicating professionally. Lastly, P01 offered some new insight through his explanation that he uses X/Twitter and Instagram for voicing political opinions.

Wellbeing, Social Comparison and Time Displacement

Wellbeing research is increasingly ambiguous and nuanced. Passive social media use and comparison have been correlated with low levels of wellbeing and/or depressive symptoms and loneliness (Kross et al., 2013; Primack et al., 2017; Shakya and Christakis, 2017; Hunt et al., 2018). There is also evidence from experimental and longitudinal studies that passive use negatively affects wellbeing, and restricting social media use reduces loneliness or depressive symptoms (Verduyn et al., 2015; Hunt et al., 2018). On the other hand, recent large-scale and review-based studies argue against overly negative statements about the effects of social media use. Vuorre and Przybylski (2024) find that Internet use-associated harm is not that simple, and Sametoglu, Pelt and Bartels (2025) find complex connections between social media usage frequency, wellbeing and depressive symptoms.

In this pilot study, the important element here is the fact that wellbeing tension is situational. The participants did not view social media as negative in its totality; rather, they saw the negatives such as loss of time, loss of productivity, comparison, distraction/anxiety together with positive aspects of social media. This is shown by the participant P03's case study about his loss of concentration after watching videos and reels, P04's case study where he wanted to spend more time with actual people and P02's case study where she had two weeks away from social media. It is evident that wellbeing is experienced as tension rather than a result.

Algorithmic Datafication, Targeted Advertising and AI-Driven Personalisation

A major recent shift in the literature concerns algorithmic datafication: it is not just about hosting the activity of users; rather, it involves inferring, ranking, personalizing, recommending, and monetizing such activities by using algorithms. In research around online behavioural advertising, it has been observed that people consider personalization to be a service which is helpful yet invasive (Aguirre et al., 2015; Smit, Van Noort and Voorveld, 2014; Boerman, Kruikemeier and Zuiderveen Borgesius, 2017). Participants kept referring to targeted advertising through searches, conversations, or interactions with content.

Studies on algorithmic awareness are becoming more pertinent in the context under consideration. Oeldorf-Hirsch and Neubaum (2023) suggest that the level of algorithmic awareness is related to certain attitudes and behaviours exhibited by social media users, whereas Bartol (2025) has proved that algorithmic awareness and knowledge have something to do with digital inequalities. Both studies corroborate the findings of the pilot study's Q11:

users wanted better practices at a personal level, but they also demanded transparency, minimization, privacy, independent audits, and accountability from algorithms.

Misinformation, Trust and Information Integrity

Misinformation is another significant concern because besides affecting personal privacy, it also impacts societal knowledge and trust. Research finds that false news travels widely on the internet and that affordances of digital platforms influence both the diffusion of and response to such news (Vosoughi, Roy and Aral, 2018; Guess, Nagler and Tucker, 2019; Grinberg et al., 2019; Pennycook and Rand, 2019). Within the current pilot research, misinformation came up in various ways: P03 reported fake news and conspiracy theories, P04 was sceptical about news on Facebook, P05 was concerned about AI-produced content and deepfakes, while P06 saw misinformation as a standard platform risk.

This takes the study out of the realm of privacy. Ethical issues concern the user's data privacy but also extends to information integrity within the digital ecosystem. Participants found risks across various dimensions: physical well-being, social interactions, mental health, societal discourse, and platform policy. This makes the DBA's significance of the chosen topic more relevant.

Research Gap and Contribution

There has been significant empirical evidence in the literature on privacy concerns, disclosure, well-being, misinformation, advertising, and continued use. However, much of this evidence is quantitative and focused on outcomes. Not enough research has been done into the personal explanation of users, i.e., the processes of reconciliation through which they justify their contradictory behaviours, including what justifies their continued usage, what justifications they give to themselves, how they cope with any negative feelings associated with their usage, and who takes responsibility for that behaviour.

In this regard, this paper contributes by demonstrating the layers of social media risk reconciliation. Individual strategies include passwords, 2FA, privacy settings, limiting the amount of information disclosed, limited post frequency, and careful selection of the social media platforms used. The relational aspect involves continuing usage to maintain family, friend, community, and professional networks on the platforms. The structural dimension includes understanding that one cannot solve problems such as data harvesting, black box algorithms, and engagement-based design through individual action alone.

Synthesis of the Literature for the Present Study

However, from the existing literature, it is evident that sustained social media usage cannot be described in terms of one specific theory. For example, according to the privacy calculus theory, the reason is that people assess risks versus rewards when it comes to decision making. On the other hand, contextual integrity theory offers an understanding of why the audience matters, why the context of usage matters, and why the flow of information is also significant. As for the uses and gratifications theory, it sheds light on why people repeatedly use the platform. Moreover, in relation to digital resignation theory, it provides an understanding of why some people feel uneasy about using social media but continue using them. Finally, wellbeing literature explains how the outcomes of social media depend on its nature and context.

From this analysis, the interpretive nature of the study becomes clear. It does not focus on whether social media is good or bad. Instead, it asks the following question: "How do people construct meanings amid contradictory conditions?". In this regard, the idea of reconciliation becomes crucial because it means that there is no way that users will be able to reconcile everything at once. This literature review makes an important contribution toward informing the study's theoretical foundations and directions. Given that participants' decision-making process is informed by factors such as platform defaults, social pressure, algorithmic opacity, and lack of options, individual users cannot be expected to shoulder the blame. As a result, the findings from the literature review suggest that the next step should be an examination of protective practices, rationalizations and recommendations from Q11.

The conceptual framework that emerges from the literature may be stated as follows: the users stay engaged since the platforms deliver significant gratification and social capital to them; at the same time, they become anxious over the issues of privacy, well-being and misinformation; the latter two are reconciled by means of boundary-making, selective disclosure and rationalisation of choices. It is particularly fitting for a pilot study to use such a theoretical framework, since it gives rise to concepts that focus researchers' attention but do not restrict participants' meaning-making processes.

It becomes clear from the literature review why the project under consideration also has a business management and policy component. Platform corporations exercise considerable influence on users through such means as default settings, interface design, recommendation systems, ad models and reporting functions. Regulatory authorities create the environment

within which platform corporations operate and through which users are supposed to navigate as well.

Another implication emerging from the literature concerns the distributed nature of responsibility. Individuals can set the terms and limit their disclosure using privacy settings; however, the platform influences what options are available and the ease of adopting safer practices. Finally, regulation is needed to determine whether the responsibilities of the platform are voluntary or mandatory. In such circumstances, the reconciliation of individuals can be seen as more than a personal compromise.

Hence, this literature review forms the theoretical foundation for the findings. It helps understand why people keep on using services despite their concerns, why privacy protection is partial and how well-being impacts depend on context. Moreover, it supports the significance of participants' demands for transparency and regulation in theory. Finally, the literature review explains the choice made to focus specifically on the accounts of ordinary users.

Methodology

Research Approval

This research took place following the approval of the PG2 Research Ethics Form from the supervisor. Prior to collecting data, the Participant Information Sheet and Consent Form were sent to each participant via email. These contained information about the purpose of this study, voluntary participation, procedure, anonymisation, the option to refuse answering any question, and withdrawal prior to anonymisation. The participants provided signed Consent Forms via email prior to participating in the interviews. Participants were coded P01-P06 in all transcripts, audit trail, analysis and the report.

The project did not ask for the participants' passwords, access to any private accounts, screenshots of accounts, or other sensitive information. The interviews prompted participants to think about their typical social media usage and associated perceived risks, protective measures taken, and responsibilities of platforms, regulators, and individual users. The signed consent forms and the study materials were safely kept away from the anonymised analysis documents. Quotes used in the study were anonymised, particularly when discussing professional identity, politics, fraud, wellbeing, and international relations.

Research Approach

An interpretivist qualitative methodology was applied to this study because of its intention to explore the meaning-making of social media risk. Interpretivism is a valid choice of methodology if a researcher is concerned with subjective meanings, experience, and processes of interpretation employed by participants when talking about themselves and their actions (Crotty, 1998; Bryman & Bell, 2015). It is relevant for the present research since the investigation intends to identify where risk tension arises, how it is interpreted, and which practices or rationales help to cope with this tension.

A coherent methodology can be defined as a consistent combination of interpretivism with a qualitative pilot study, semi-structured interviews, individual-level reflexive thematic analysis, and cross-case identification of themes. Positivistic notions of generalisability, hypothesis testing, or inter-rater reliability do not appear in the report. Methodological quality is determined through coding transparency, reflexivity in making decisions during coding and analysis, providing an audit trail, and linking the research questions, interview questions, data, and themes produced.

Research Design

The research design was an exploratory qualitative pilot study. A pilot design was suitable since the aim was to examine whether the research topic, interview guide, participant recruitment and analysis were viable before carrying out the main study. The advantages of conducting pilot studies are that they help researchers know whether their participants can adequately answer questions raised, whether the questions posed lead to generation of appropriate data and whether the analysis strategy is plausible (van Teijlingen & Hundley, 2001; Kim, 2011). In this case, the pilot demonstrated that the participants could discuss issues of privacy, well-being, scams, datafication, misinformation, platform dependence and ethical dilemma. Semi-structured interviews were conducted since they offered adequate consistency among the participants while allowing individual examples and meanings as well as probes from the researcher (Brinkmann & Kvale, 2015; King & Horrocks, 2010). The same key areas were explored across P01-P06; however, each of them stressed different topics including political activism for P01, invisible data profiling and social entanglement for P02, Facebook/Messenger use and scam links for P03, relational dependency and self-censorship for P04, low use intentionally and AI/datafication for P05, and professional and banking scams for P06.

Participant Selection and Recruitment

The participants were recruited using a purposive sampling procedure aided by convenient access to individuals via social and professional networks. It was important to choose purposive sampling since the study needed adults with sufficient experience using social media to be able to reflect upon the risks, benefits and sustained usage (Patton, 2015). The inclusion criteria for the participants were as follows: being at least 18 years old, having experience of using social media in an engaging manner and discussing topics related to privacy, wellbeing, ethical dilemmas and protective actions in interviews/online surveys.

Six participants were recruited and assigned labels as P01 to P06. The size of this sample was considered adequate for a pilot study where the aim was exploratory in nature rather than being representative and aimed at developing thematic analysis. Furthermore, the diversity of platforms chosen provided sufficient variability for analysing how the concept of risk resolution depends on platform ecologies, which allowed illustrating how professional networking on LinkedIn was different from family relationships on Facebook, visibility on Instagram, political messaging on X/Twitter, etc.

Data Collection Procedures

Interviews were conducted using a semi-structured interview questionnaire along with a further written or post-interview follow-up question. Questions for interviews were based on the interview question matrix that had been prepared based on the literature review. Initial questions were focused on platform usage, benefits, risks involved. Mid-questions were based on conflict situations, benefits-risk assessment, privacy issues and wellbeing issues, rationalizations, and continuation with social media usage.

The follow-up question (Q11) was about what needed to change in the platforms, regulatory environment, or the participant themselves for the privacy/wellbeing conflicts to become more comfortable. This question enhanced the practical contribution of the study as the discussion went beyond individual coping mechanisms. Through audit trails, follow-up question number eleven produced significant discussions regarding algorithmic transparency, actual data control, improved default settings, wellbeing-based design, reduction in addictive features, independent audits, regulation, digital literacy, and mindful social media behaviour

The interviews were transcribed verbatim and coded as individual Word documents for each participant. The type of transcription used reflects the nature of the research, which focuses on the meaning process, not neat questionnaire-type answers. This involved highlighted

transcripts, memo columns, and audit trail documents per participant to capture the movement from extract to code, from code to category, and from category to tentative groups.

Data Analysis

Data analysis used Braun & Clarke-type reflexive thematic analysis (Braun & Clarke, 2006; 2019; 2022). Reflexive thematic analysis was appropriate because it attempted to develop structured meaning from qualitative data whilst being mindful of the active construction of themes through the process of engaging with data. The new P01-P06 analysis is much more reflexive than the old one as it highlights the participant level of thematic coding prior to the generation of themes across all cases.

Analysis was done through six main stages. Firstly, each transcript and Q11 addendum was read several times. The new participant documents have notes on reflective familiarisation, which highlight interesting moments, contradictions and surprises. Secondly, semantic and latent codes were developed. Semantic codes were directly related to the participant statements like “strong password”, “fake account”, “Messenger”, “targeted ads”, “no live posting”, “false birthday”, “phone avoidance” and “LinkedIn”. The latent codes reflected on deeper underlying themes, for example: controlled visibility, dependence on networks, digital resignation, right use logic, prevention first behaviour and platform power.

Third, each participant document now includes a consolidated master code list, which was a significant step since it provides an intermediary Phase 2 output before themes are produced. Fourth, the codes were organized into categories and provisional participant-level groupings. To give just a few examples: P01 identified categories of political voice, hostile visibility, and controlled visibility; P02 identified social infrastructure, invisible data profile and symbolic control; P03 identified Facebook infrastructure, scams and responsible use; P04 identified relational infrastructure, self-protection censorship and resignation from the platform; P05 identified low exposure intentional use and AI/datafication anxiety; and P06 identified communication dependency, LinkedIn necessity and responsible use logic.

Fifth, these provisional categories were examined in each participant case. As can be seen from the wording, the categories are provisional because one document cannot provide a conclusive theme. And lastly, these participant-level groupings were compared across P01-P06 to produce the cross-case themes discussed in the findings section below. This cross-case comparison is crucial for Braun & Clarke's approach: the report does not simply provide information for each participant separately but develops a coherent thematic argument across cases.

Quality and Rigour

Trustworthiness criteria developed by Lincoln and Guba (1985) were utilized in addressing quality: credibility, transferability, dependability and confirmability. Credibility was increased by conducting an analysis close to participants' examples while at the same time interpreting their deeper meanings. In particular, the updated P01-P06 audit trails are key for increasing credibility as they reflect on how familiarity reflections, master codes, categories, and provisional groups were developed prior to developing the results.

Transferability has been increased through a thick description of platforms and differences among individual participants. The report is not trying to suggest that the sample of six participants represents all social media users. Instead, it gives the reader sufficient information on whether the analysis might also apply to other users in similar online environments. Dependability has been achieved via the use of audit trail, colour coding, code tables, master code lists, definition of provisional groups and cross case comparison. Confirmability has been achieved via reflective statements and preservation of data supporting an anti-social media interpretation such as politics, family, career development, learning, professional networking and ethical participation.

Reflexivity and Pilot Limitations

Reflexivity was required due to researcher's pre-existing interest in ethical tension and issues of privacy and platform accountability. This could result in bias towards risk. It was therefore important for the analysis to retain positive factors for continued use and categorize forms of continued use. P05 who is a low-user, P06 who uses LinkedIn professionally, P04 who is dependent relationally, P03 who communicates via Facebook, P02 who is socially entangled and P01 who voices politically are all indications of meaningful reasons behind continued use.

Limitations of the study include the small sample size, convenience sampling, use of self-reported data and lack of depth in some interviews. Q11 was conducted after the interview proper, hence its inclusion in the data set as reflective data rather than spontaneous discussion during an interview. These limitations are appropriate for a pilot study and have been addressed in the analysis. Improvements for future research include more probing on ethical tension and more follow-up questions and possibly even comparing users by age group or platform type/usage intensity.

Data Management and Audit Trail

The data corpus comprised six analysis/audit-trail documents, along with their associated coded transcripts. Participant codes were utilized in all cases to protect confidentiality. The revised audit-trail documents clearly document the analysis process in full detail: colour code key; database description; reflexivity statement; Phase 1 familiarization memo; Phase 1a reflective familiarization; Phase 2 initial coding; Phase 2a master code list; Phase 3 code-category-grouping logic; Phase 4 initial review; Phase 5 provisional definition and Phase 6 illustration.

The audit trail is significant in that it enables the reader to understand how the final themes have been generated. For instance, the theme "social media infrastructure" stems from participant P01's political voice, P02's social loop, P03's Facebook/Messenger reliance, P04's international relationships, P05's tangible connection and P06's communication and professional use. In a similar way, the theme "structural responsibility" emerges out of the repetitive response to Question 11 about the need for transparency and regulation, default privacy, algorithms and digital literacy.

Methodological Learning from the Pilot

Methodologically, the pilot interview delivered four key insights. The first is that the interview guide worked well because it provided information about privacy, well-being, scams, datafication, misinformation, continued use, and change. The second insight is that the notion of ethical tension required more clear explanation, indicating that in future interviews the notion should be introduced more succinctly. The third insight is that the Q11 question following the interview was important because it enhanced the practice-focused approach of the research, enabling the respondents to progress from individual coping to platform and regulation responsibility. Lastly, an audit trail per participant confirmed the importance of postponing the decision to select themes until the end of the process.

Findings: Emergent Data Observations and Deductions

Final findings were generated through cross-case analysis of the preliminary categorizations P01 to P06. Participant level texts reveal that each case possessed its own logic of reconciliation: controlled visibility for protection of voice (P01); social entanglements and symbolic control (P02); Facebook as infrastructure of communication and management of risks (P03); maintaining distance with protective self-censorship (P04); minimization of exposure through selective usage (P05); and justification of social media usage for communication,

learning and work (P06). Six major cross-case themes were derived from these varying logics of reconciliation.

Theme 1: Social media functions as social, professional, communicative and moral infrastructure

The first theme refers to the continued use of social media because such platforms serve an infrastructural purpose within meaningful daily functions. P01's story best exemplifies moral and political infrastructure as X/Twitter and Instagram allow public speech and advocacy. For P02, social media is the way into the ongoing process of news about events, group conversations, opportunities, and belongingness. The story from P03 highlights Facebook and Messenger as infrastructures of everyday communication, specifically in the Bangladesh setting. As stated by P04, Facebook and Instagram are used for connecting with family members, old friends, colleagues, and foreigners; meanwhile, according to P06, WhatsApp, Messenger, and LinkedIn are the infrastructures of communication and professionalism. Even P05, despite his limited experience as a user, keeps Facebook and LinkedIn, as those social networks still prove to be helpful in terms of communication, news, education, and professionalism.

It relates to RQ1 since it illustrates how the risk tension appears within the context of infrastructures that help users to connect with their families, establish their career, publicly speak out, get informed, and communicate with others.

Theme 2: Risk becomes meaningful when it is concrete, visible or emotionally close

All participants identified general threats ranging from privacy breaches, scams, hacking, misinformation, data gathering, wastage of time, and potential wellbeing threats. It appears that the risk only becomes real when it relates to a specific experience or something closer to the user personally. The fake account and dox threat mentioned by P02 made privacy risk more relational. P03 experienced suspicious links and gambling redirects which turned the general privacy risk into a practical precaution.

The hacking of her email, lockout from her account, and unwanted picture sharing experienced by P04 make the privacy risk unforgettable. The financial threats faced by P06 related to banking fraud and social media exposure.

While P05 had not experienced any major harm, targeted advertisement, misinformation generated by AI technology, and scamming of their friends/colleagues made them cautious. In the case of P01, there is another type of concrete risk: hostile visibility. Risk becomes real through harassment, racism, being banned from the platform, vulnerability to reputation or job losses, and even censorship of political speech.

Theme 3: Reconciliation is a relational, emotional and practical privacy calculus

These results are consistent with Privacy Calculus Theory because individuals constantly engage in a trade-off between risks and rewards. Nevertheless, the participant-based audit trail suggests that it was far from rational thinking involved in this process. Thus, P02 explicitly mentions poor reasoning such as "all boats are sinking together" and "have nothing to hide" as tools to suppress feelings of guilt. P04 accepts the risk of using social media because the alternative could involve cutting off oneself from valuable personal connections. Meanwhile, P01 justified exposure because having a voice in politics is a moral obligation. P03 employs the idea of a "responsible tool" for continuing to use social media, while P06 applies a "right-use principle" – social networking is helpful if one uses it responsibly.

This theme provides an answer to RQ2 as it indicates that ethical tensions cannot be overcome permanently. They are managed through continuous justification in terms of balancing privacy and connection, risk of exposure, convenience, and gained knowledge, and even discomfort and career or family communication.

Theme 4: Protective practices create partial, sometimes symbolic, control

Every participant provided examples of protective measures. This included the usage of pseudonyms, fake or obscured birth dates, general location, lack of any live posts, no pictures of family members or vehicle number plates, strong passwords, two-step verification, privacy settings, private account, limited audience, contact-only audience, avoiding suspicious links, reduction of phone usage, settings checks, and non-discussion of political and religious affiliations. These measures enable the participants to keep using social media platforms without being too reckless.

The findings of this study reveal that protective control is always incomplete. The participant P02's metaphor of lock on the door with glass panels perfectly illustrates this. Participant P04 feels that usage of privacy policy is necessary for continuous use of Facebook. Participant P05 avoids using phones when on the app as she believes that background tracking cannot be

avoided when using an app. Similarly, even though Participant P01 uses a pseudonym to protect her identity, the possibility of abuse remains.

Theme 5: Risk awareness usually produces cautious adaptation rather than full withdrawal

Overall, awareness of risk influenced behaviour but did not result in full-scale withdrawal from the social media. For example, P01 left Facebook but remained an active user of X/Twitter and Instagram for political reasons. Similarly, P02 closed their account at Facebook but understood that risks are now relocated to other social media platforms like Instagram and Tiktok. P03 began using social media more selectively and intentionally; he scrolled less often and started communicating using Facebook for informative purposes. P04 became more cautious and stopped live postings and controversial statements, spending more time outside and with "real people". Lastly, P05 used social media in a more controlled manner. P06 used less Facebook when transitioning from university to professional life.

The finding is directly related to RQ3, as participants mitigate risks through moderation, migration, selective disclosure, compartmentalization, and social media-specific use. This finding is crucial since it disproves the common myth that awareness should necessarily result in abandoning a particular social medium or practice

Theme 6: Ethical comfort requires platform and regulatory responsibility as well as individual mindfulness

The Q11 follow-up showed an evident cross-case theme. Individuals were sure that their willpower was not enough to resolve social media risks. P01 stressed the importance of platform accountability, engagement economy, algorithmic transparency, regulation, and digital literacy. P02 insisted on having more data sovereignty, transparency, and regulation that would consider users' wellbeing more than the profitability of firms. P03 advocated for the improvement of algorithmic transparency, privacy regulation, elimination of addictive designs, and healthy user behaviour. P04 recommended platforms to focus on well-being over engagement, offer enhanced privacy by default, and follow more severe data protection regulations. P05 demanded privacy and well-being by default, data minimization, external algorithm audits, and international standards. P06 stressed the importance of platform transparency, regulation, and mindful personal usage.

As cross-case analysis demonstrates, the participants were ready to admit individual responsibility, yet they rejected a single-individual approach. The responsible ethical use of

social media required multi-level responsibility from platforms, regulatory agencies, and individuals themselves.

Cross-Theme Deduction

In general, this study has shown that risk awareness and sustained platform usage is a multilevel phenomenon. Participants recognize risks, derive value, adopt precautionary measures, make sense of using platforms, modify their behaviour accordingly, and even demand structural changes. The main finding from the pilot study is not about the risks involved when using social media because those have been discussed sufficiently in academic literature before. The important findings are regarding what users do with social media despite recognizing these risks.

Cross-Participant Data Matrix

Participant	Distinctive provisional grouping emphasis	Main driver of continued use	Main risk/ethical tension	Protection/adaptation	Q11/systemic change view
P01	Political voice, hostile visibility, controlled visibility.	Advocacy, political expression and awareness raising through X/Twitter and Instagram	Abuse, racism, account closure, reputational/professional exposure and platform silencing	Pseudonymity, no family/name/location details, identity compartmentalisation and selective Facebook withdrawal	Algorithmic transparency, regulation and digital literacy
P02	Social infrastructure, invisible data profiles, personal incidents, guilt and symbolic control	Being in the loop, social belonging, friends, news, opportunities and real-time updates	Invisible profiling, impersonation, doxing, targeted ads, manipulation and social cost of leaving	Private accounts, false birthday, location off, privacy checks, password changes and migration rather than exit	Genuine data control, stronger laws and systemic support beyond individual willpower
P03	Facebook infrastructure, scam encounters, attention loss, and shared responsibility	Facebook/Messenger communication, family connection, learning, entertainment and business ideas	Scam links, betting redirects, data misuse, time loss, fake news and productivity loss	Strong passwords, 2FA, privacy settings, audience limits, vague location and reduced scrolling	Algorithm/data transparency, reduced addictive features, privacy laws and healthier habits
P04	Relational infrastructure, persistent risk, protective self-censorship and	Relationships with family, old friends, colleagues and people abroad; peace of mind	Hacking, photo misuse, fake news, time loss, targeted ads, data extraction and accept-or-exit privacy policies	No live posting, hidden DOB, known contacts, limited personal detail, privacy reviews and	Wellbeing-led design, default privacy, transparent algorithms and stricter

	surveillance resignation			avoiding controversy	data protection
P05	Low-use identity, practical benefits, invisible datafication/AI and prevention-first selectivity	Limited connection, messaging, updates, learning and LinkedIn/professional information	Background data collection, targeted ads, AI-generated misinformation, deepfakes, tracking and time loss	Limited/passive use, information minimisation, privacy settings, laptop use, private profiles and prevention-before-repair	Privacy and wellbeing as defaults, data minimisation, independent algorithm audits and standards
P06	Communication dependency, LinkedIn professional necessity, fraud/hacking risk and right-use logic	WhatsApp/Messenger communication, friends/family abroad, learning and LinkedIn career usefulness	Hacked accounts, banking fraud, scams, misinformation, targeted advertising and data sharing	2FA, strong passwords, suspicious-link caution, private settings, known contacts and reduced disclosure	Transparent data practices, stronger regulation and mindful screen time/sharing
P04	Relational infrastructure, persistent risk, protective self-censorship and surveillance resignation	Relationships with family, old friends, colleagues and people abroad; peace of mind	Hacking, photo misuse, fake news, time loss, targeted ads, data extraction and accept-or-exit privacy policies	No live posting, hidden DOB, known contacts, limited personal detail, privacy reviews and avoiding controversy	Wellbeing-led design, default privacy, transparent algorithms and stricter data protection

Thematic Map

Map element	Analytical meaning in the revised report
Central phenomenon	Risk-aware continued platform use: participants remain online while recognising privacy, wellbeing, data, misinformation and platform-power risks.
Driver layer	Social media functions as infrastructure: political voice (P01), social loop (P02), Facebook/Messenger communication (P03), relationships abroad (P04), controlled practical use (P05), and communication/professional networking (P06).
Risk layer	Risk becomes meaningful when concrete: hostile visibility, impersonation, doxing, scams, hacking, photo misuse, targeted ads, AI misinformation, fraud and data commercialisation.
Reconciliation layer	Participants use emotional, relational and practical calculations: benefits outweigh risks, right-use logic, responsible tool narrative, limited-use identity, guilt quieting and connection over withdrawal.
Management layer	Risk is managed through partial control: pseudonymity, privacy settings, 2FA, strong passwords, no live posting, reduced disclosure, selective platform use, self-censorship and prevention-first behaviour.

Adaptation layer	Awareness usually leads to cautious adaptation, platform migration, moderation, intentional use or reduced exposure rather than full withdrawal.
Structural layer	Ethical comfort requires platform transparency, default privacy, algorithmic accountability, stronger regulation, reduced addictive design and user digital literacy.

Conclusion: Contributions, Limitations and Recommendations

This pilot study sought to examine how users negotiate awareness of issues such as privacy, wellbeing, data and ethics against their continuation of social media platform use. In light of the changes made to the analysis through P01 to P06 audit trail documents, it is evident that users continue using platforms not because they lack awareness but rather because social media platforms are intertwined into processes of communicating, connecting with family, building networks for work, expressing political views, learning, accessing information and socializing.

Contributions

The main theoretical contribution is an extension of the debate regarding the privacy calculus and privacy paradox. This study supports the notion that users engage in weighing benefits against risks; however, it indicates that such weighing is far from rational. User choices and behaviours are determined by moral motivation, dependence on the platform, usefulness of the platform, fears of ostracism, convenience, guilt avoidance, and limitations imposed by dependency. The main empirical contribution is a cross-case discussion of reconciliation. P01 explains how the need for political voice justifies controlled visibility. P02 explains how social infrastructure and practices of symbolic privacy make users continue using platforms. P03 explains how the balance between communicating on Facebook/Messenger and avoiding scams and inattentiveness keeps users using platforms. P04 explains how dependence and self-protection lead to communication censorship. P05 explains the use of low-exposure Facebook/Instagram due to datafication and fear of AI. P06 explains the management of communication and professional worth via cautious use. These cases prove that continued usage does not require ignoring issues but awareness and adaptation.

The second methodological contribution is the enhanced Braun and Clarke audit trail. It now includes reflective familiarisation, a unified list of codes, grouping from code to category, provisional categories, and illustrative write-up for each participant. It allows a stronger credibility of final themes because one sees how codes turned into participant-level categories and then cross-case themes.

Limitations

Limitations include the small-scale pilot study involving only six individuals, and convenience sampling. Findings cannot be generalized as a statistical sample representative of all social media users. Self-reports may also have resulted in participants having perceptions about their own privacy behaviour or changes in usage time that differ from objective measurements of digital footprint. Some interview questions needed to be elaborated upon, notably the use of the term "ethical tension."

Another limitation stems from Q11, which was inserted as an additional question based on academic review feedback. While it made the research contribution more practically relevant to the DBA program, the responses to this question may not have been quite as spontaneous as interview discussion. Additionally, there is some element of researcher interpretation involved in the categorization process; another researcher may have reached alternative but equally justifiable conclusions.

Recommendations

For individuals who practice using the technology, it seems evident that responsibility towards the problem of safer social media should be shared. Individuals need to keep following the recommendations such as using strong passwords, enabling two-factor authentication, implementing privacy settings, being cautious about the sharing of their personal information, controlling audiences, limiting locations, establishing clear rules about screen time, and avoiding clicking suspicious links. On the other hand, the study demonstrates that these measures are not enough if the system of the platforms is not understandable to users, highly manipulative, and commercialized because of its dependence on the gathering and usage of data. Thus, platforms need to start communicating more clearly with regard to the process of data gathering, giving users an opportunity to control it and have default settings that will protect the users' personal data better; at the same time, it is necessary to improve the algorithms, stop being manipulative, and provide users with opportunities to prevent the usage of their accounts for various types of harassment or impersonation.

Overall, the pilot indicates the potential of the topic to be viable for further DBA research. The interview guide was effective at producing quality data, Q11 provided additional practical contribution, and the modified audit trail provides a solid framework for transitioning from the extracts to cross-case themes.

Part C: Reflection on Personal Learning and Skill Development

The pilot study provided me with an insight into the reflexive nature of qualitative research. In the initial stage of the research process, I approached the interview guide as a set of questions that needed to be completed. P01-P06 audit trails in their revised form provided valuable insight in terms of a more structured approach needed when conducting qualitative analysis from familiarisation to codes, categories, and provisional groupings.

Dr. Caroline's comments were very helpful as she demonstrated how reflective notes on familiarization need to be and Q11 follow-up question for post interview. In the revised forms, I therefore focused on identifying what was surprising about each participant case, any tensions involved, and what made me think. For example, the case of P05 who used the network to a lesser degree, as well as P06's professional usage of LinkedIn.

The coding process further developed my analytical skills. Having lists of master codes for both phases kept Phase 2 more tangible and helped avoid prematurely going into themes. It was useful to realize that a good theme is not just another name for a topic like "privacy" or "risks". Good themes make arguments, e.g., "protective practices provide partial and sometimes merely symbolic control" or "risk awareness leads to cautious adaptation and not withdrawal".

Lastly, conducting pilots is a worthwhile practice since it not only shows where methodological weaknesses lie but also highlights findings. Q11 follow-up interviews helped develop the practical aspect of the study, while creating the audit trail improved its transparency. For future interviews, I will make sure to have clear definitions of terms, explore participants' strong examples in depth, and use participant audit trails.

As for the theoretical implications, this pilot study increased my knowledge about qualitative research. Initially, I viewed the interview guide as something to ask a list of questions on. However, during analysis, I realized that one should listen actively while interviewing and try to probe participants about the information they provided. Indeed, some transcripts indicate that at times I failed to probe participants thoroughly enough after receiving a good answer or simply asked the same question again.

Finally, the coding phase improved my analysis skills. Although the three-colour coding was helpful in terms of managing information, the audit-trail documentation prepared by Braun and Clarke made it clear that coding is just a first step. It is more important to move on to categories

and then to themes. One should remember that a theme should not just name something, e.g. “privacy” or “risk”. A good theme makes an argument; for instance, protective practices provide partial and symbolic control.

It is also important to consider that of reflexivity. Risk is the main aspect my research is centred around, which means I could have tended to be biased about negative factors associated with the use of social media. However, those involved have reminded me that there are always valid reasons why people continue using social media such as connection to one’s family, voice in politics, finding jobs, and learning purposes. The pilot study has shown the significance of having an audit trail.

Appendices

Appendix A: Raw Interview Transcript

Speaker	Dialogue	Memos / Notes
Interviewer	So, first of all, which social media platform do you use frequently?	
Participant 01	Many times a day I use X, Twitter, and Instagram. So if I post on X, then I share on Instagram. So I think they're quite different platforms. I have a Facebook account that I haven't used for, say, 10 years. Sometimes I use it to look for photographs of a friend or to see if there is this radio programme I listen to and they put the synopses, but I wouldn't say I never post on it, but I might have a look at one or two things, very rare.	
Interviewer	Can you tell me how you typically use social media in your daily life?	
Participant 01	So I largely use social media to be politically active for things that are important to me. So I post at least 40 to 100 posts every day on X. Many of them are retweets, so I'm tweeting somebody else, but I do my own posts as well. My feeling about X is that it's the most appropriate source for political and news stories. If I choose to post on Instagram, what I like about Instagram is it's easy for me to put audio. It's easy for me to make an image very impactful. If I post on X, you don't need an image. Sometimes it can just be the statement, the thoughts that I have. I really don't like Facebook. Facebook is the one that, I don't know, is it the oldest one out of the ones that I use? It's just too gossipy for me. It's not as political and it's a different type of site for me. There are other social media sites that I have. I have a Substack page. I have some blog pages. I've been banned from TikTok a number of times because of my politics. LinkedIn, I've been banned from there as well. So, in answer to your question, the ones I use most frequently are X and Instagram.	
Interviewer	What kinds of risk, if any, do you think are associated with using social media, or what risks are people facing while using social media?	
Participant 01	Well, you know, I have taught management ethics at master's level and the students have done studies on the ethical tensions with social media. I don't necessarily feel I am exposed to all of them in terms of racism, sexism, homophobia. We are largely, as a population or community, becoming more and more aware that if you type something on social media, it can be there forever. Even if you delete it, somebody's got a record of it. I think a lot of people are aware of scams. I was reading on the weekend about somebody that lost millions with a romance scam. And then, you know, there are very unkind statements with keyboard warriors. Some people won't say to your face, 'you're fat and ugly', but they seem to type it. I've done some research on problem gambling and particularly online, and it's just so easy to do and so quick and so fast. All of us get stressed and often think something under our breath, but very rarely would we say it to that person's face. But we seem to have a state of dissociation. So we can type horrible things about a celebrity because we don't know them. I try very much not to do that. My biggest problem is that I use a pseudonym on social media because regarding being very pro-Palestine, there are consistently efforts to make the pro-Palestine voice quiet. I think I'm on my fourth account on Instagram because I've been closed down multiple times by people saying I'm anti-Semitic because genocide is wrong. I could give up and not open another account, but I think it's really important to me to make a noise about things that I think are heinous, really, really bad. So, social media is very dangerous in many, many ways. I've not had a scam	

	and I've not experienced lots of things that I know happen, but because I've always had an interest in ethics, maybe I'm older, a different generation, and a bit more cautious.	
Interviewer	Have you ever experienced or encountered any issues related to privacy or data while using social media?	
Participant 01	I don't know if I'm answering your question right, but I remember, say, 12 years ago, going on Facebook and there would be quizzes, like take this quiz to see which character in Harry Potter you are, take this quiz to see which rap star you are. When I was first doing these things, just passing time, I didn't realise that they were collecting information about me, about my preferences. I didn't realise initially, but as soon as I did realise, and I think my son, when he first went to medical school, I took a photograph with him and I posted it on Instagram. Immediately I had comments from persons affiliated with Israel saying things like, 'fat, ugly mother with a really ugly son.' That happened once and it didn't happen again. I never post anymore because some people are crazy, but many, many more people are very unkind. Regarding privacy, there are certain countries where you are paid to look at the internet and respond to people who are anti-Israel. I am anti-Israel. It's very dangerous, but when I was about 14 or 15, I was on demonstrations to free Nelson Mandela, so I've always had a political leaning and I'm not going to change now. Regarding privacy, I'm careful. I didn't realise initially about privacy, but I would never post my car with a number plate, my son's car, nothing. I'm quite careful now.	
Interviewer	Do you ever feel conflicted about using social media?	
Participant 01	Well, yes. There are a couple of things. First of all, I do spend a lot of time posting. It's not hours and hours, but I probably spend one or two hours a day posting or sharing posts because this is a political issue I think is really, really important. Number one, it's the time that I know maybe I could be doing other things. The other thing is I know that there's an element of danger because a number of academics from other universities have been sacked for supporting Palestine. So that's why I don't put my name. But I think if I am careful, the problems are outweighed by the positives. Sharing messages and sharing information in a sensible way has risks, but you know me a little bit, Marvin. I am not the quiet type. If I see something is wrong or something is good, if I can do anything to help anyone, I will. Life changes, and when I was your age, there was no social media. My mother said the biggest change in her life was the internet. It is a wonderful, wonderful tool. Look what we are doing now because of digital technology. So we have to be careful of absolutely everything, but if you were super, super, super careful and worried, then you wouldn't even leave the house. It's all about managing benefits and risks. Nothing is without risk.	
Interviewer	Even when you are aware of the risks, what keeps you using social media?	
Participant 01	Regarding Facebook, which I have an account but I don't use, I stopped using that because I saw bullying on it. My son was bullied on it. There was a lot of racism towards my son. People would post a picture of their house, their holiday, their next holiday, their new car. I'm not unhappy for them, but I don't really want people to see my new car or my new house or my new dog or my new boyfriend, not that I have one. I found that quite stressful because people tend to show you something and maybe it's not real. That is the big thing for me with Facebook. I don't like it. I really, really don't like it. But I am very, very passionate about some political issues, and Twitter or X and Instagram allow me to make some noise, create awareness, show my passion and show my concern for a very disadvantaged	

	population. Where we are in 2026, when I see injustice, social media for me is a way to contribute to the debate, create awareness and chat with like-minded people. So yes, the risks are there and the risks are serious, but it is a channel that has opportunities for me to share messages about political issues.	
Interviewer	How do you weigh the benefits of social media against the potential risks?	
Participant 01	It's really stuff I've already mentioned, but there are risks to everything. There are some people who are not politically interested, people who don't vote. I'm not one of these people. I think it goes back to my first degree in philosophy and a master's in political philosophy. It is something that I'm very, very interested in. When I started on social media, on Twitter, maybe I had three followers, then ten followers, then 100 followers, and I've got about 2,000 now. That is not two million or 200,000, but some people follow me and I follow people. It's not that it gives me a buzz, but it means that my message is getting out and I'm seeing similar posts regarding a particular issue that is very important to me.	
Interviewer	What do you tell yourself to justify continuing to use social media despite being aware of the risks?	
Participant 01	I say something very unusual, if you like. I believe that the right situation is eventually shown. If I don't have hope, there's no point spending two hours a night posting for Palestine. But I believe that this, just like apartheid in South Africa, ultimately will be recognised globally as wrong. That is the only thing that keeps me going. If I think about racial segregation in America and apartheid in South Africa, eventually the right and moral side won. That is what keeps me going. I'm always mindful not to disclose any personal information. I may mention Wales and Bahrain, but I wouldn't go into detail for fear of retaliation or trouble.	
Interviewer	Do you take any steps to protect yourself from risk when using social media? Can you give me an example?	
Participant 01	I think, like I say, I don't use my name or family name. I don't post images or photographs of myself or my family. I don't post locations. Regarding social media, I wouldn't say these are just basic. I've just had so many accounts closed by sharing a post from Al Jazeera News. TikTok have shut me down twice, Instagram four times, LinkedIn once, and I'm just sharing that there has been a massacre of, say, 176 children. It's an incredibly powerful agenda. So the steps I take are not using my real name, not showing family, not showing locations and not giving people information that could connect my political views back to my private life.	
Interviewer	How do you manage your privacy or personal information on social media?	
Participant 01	I'm as vague as possible. So I lie about my date of birth. I removed 10 years. I don't use my name. I'm very vague.	
Interviewer	Have your social media habits changed over time because of the risks that you have already shared?	
Participant 01	I've kind of silently withdrawn from Facebook. One reason I still have it is that some old friends of mine from university are on Facebook and they live in Australia. I don't know their home addresses or telephone numbers. But I don't post at all and I don't follow my children either. Ultimately, I believe that awareness of problems, awareness of situations and spreading awareness is really important. As long as I don't give too much information away, where I work,	

	who my husband is, then it is just managing risks like you would with any kind of risky activity. I don't know anybody who doesn't have a social media account. My mother is on Facebook all the bloody time and she is 84. My sons are on Snapchat. It is now part of life. Instead of things being on television, information is so quick. I saw the news about the Queen's husband on Instagram. It is so quick to see the Liverpool team sheet. I'm also a passionate Liverpool fan, and on Instagram you see players in training and chatting, and that gives me a great deal of pleasure. Of course, the other thing is that it's free, and I do these little speech marks because nothing is free. But at the point of contact, it's free, instant and interactive. It's just part of life. Even the university has apps. I compartmentalise my life. You have work Caroline and then you have Palestine Caroline. I want to do the right thing as much as I can. If I can do something good, I always, always will do good and not bad.	
Interviewer	Thank you, ma'am. Thank you for your time.	
Participant 01	Okay. I want you to know, you must make notes as soon as we finish. I want you to think, because sometimes we went over the same things. You never asked me, 'Can you tell me a little bit more?' You have to be more in control and you have to listen to what the participant says and always know in your mind, what do I want? If she says something and you have covered something with an earlier question, have another question, have something in your pocket. I'll see you in a couple of weeks, yes? Give my regards to Mrs Gomes.	

Appendix B: Coded Transcript

Speaker	**Dialogue**	**Memos / Notes**
Interviewer	So, first of all, which social media platform do you use frequently?	
Participant 01	Many times a day I use X, Twitter, and Instagram. So if I post on X, then I share on Instagram. So I think they're quite different platforms. I have a Facebook account that I haven't used for, say, 10 years. Sometimes I use it to look for photographs of a friend or to see if there is this radio programme, I listen to and they put the synopses, but I wouldn't say I never post on it, but I might have a look at one or two things, very rare.	Codes: platform ecology; X/Instagram as routine platforms; Facebook as residual/low-use. Category: selective platform use.
Interviewer	Can you tell me how you typically use social media in your daily life?	
Participant 01	So I largely use social media to be politically active for things that are important to me. So I post at least 40 to 100 posts every day on X. Many of them are retweets, so I'm tweeting somebody else, but I do my own posts as well. My feeling about X is that it's the most appropriate source for political and news stories. If I choose to post on Instagram, what I like about Instagram is it's easy for me to put audio. It's easy for me to make an image very impactful. If I post on X, you don't need an image. Sometimes it can just be the statement, the thoughts that I have. I really don't like Facebook. Facebook is the one that, I don't know, is it the oldest one out of the ones that I use? It's just too gossipy for me. It's not as political and it's a different type of site for me. There are other social media sites that I have. I have a Substack page. I have some blog pages. I've been banned from TikTok a number of times because of my politics. LinkedIn, I've been banned from there as well. So, in answer to your question, the ones I use most frequently are X and Instagram.	Codes: moral/political purpose; platform affordances; high-frequency posting; account closure. Category: advocacy-driven use.
Interviewer	What kinds of risk, if any, do you think are associated with using social media, or what risks are people facing while using social media?	

Speaker	Dialogue	Memos / Notes
Participant 01	Well, you know, I have taught management ethics at master's level and the students have done studies on the ethical tensions with social media. I don't necessarily feel I am exposed to all of them in terms of racism, sexism, homophobia. We are largely, as a population or community, becoming more and more aware that if you type something on social media, it can be there forever. Even if you delete it, somebody's got a record of it. I think a lot of people are aware of scams. I was reading on the weekend about somebody that lost millions with a romance scam. And then, you know, there are very unkind statements with keyboard warriors. Some people won't say to your face, 'you're fat and ugly', but they seem to type it. I've done some research on problem gambling and particularly online, and it's just so easy to do and so quick and so fast. All of us get stressed and often think something under our breath, but very rarely would we say it to that person's face. But we seem to have a state of dissociation. So we can type horrible things about a celebrity because we don't know them. I try very much not to do that. My biggest problem is that I use a pseudonym on social media because regarding being very pro-Palestine, there are consistently efforts to make the pro-Palestine voice quiet. I think I'm on my fourth account on Instagram because I've been closed down multiple times by people saying I'm anti-Semitic because genocide is wrong. I could give up and not open another account, but I think it's really important to me to make a noise about things that I think are heinous, really, really bad. So, social media is very dangerous in many, many ways. I've not had a scam and I've not experienced lots of things that I know happen, but because I've always had an interest in ethics, maybe I'm older, a different generation, and a bit more cautious.	Codes: online permanence; abuse; scams; political silencing; pseudonym. Category: risk awareness and hostile visibility.
Interviewer	Have you ever experienced or encountered any issues related to privacy or data while using social media?	
Participant 01	I don't know if I'm answering your question right, but I remember, say, 12 years ago, going on Facebook and there would be quizzes, like take this quiz to see which character in Harry Potter you are, take this quiz to see which rap star you are. When I was first doing these things, just passing time, I didn't realise that they were collecting information about me, about my preferences. I didn't realise initially, but as soon as I did realise, and I think my son, when he first went to medical school, I took a photograph with him and I posted it on Instagram. Immediately I had comments from persons affiliated with Israel saying things like, 'fat, ugly mother with a really ugly son.' That happened once and it didn't happen again. I never post anymore because some people are crazy, but many, many more people are very unkind. Regarding privacy, there are certain countries where you are paid to look at the internet and respond to people who are anti-Israel. I am anti-Israel. It's very dangerous, but when I was about 14 or 15, I was on demonstrations to free Nelson Mandela, so I've always had a political leaning and I'm not going to change now. Regarding privacy, I'm careful. I didn't realise initially about privacy, but I would never post my car with a number plate, my son's car, nothing. I'm quite careful now.	Codes: data collection; abusive comments; privacy learning; careful sharing. Category: privacy/data concern and incident memory.
Interviewer	Do you ever feel conflicted about using social media?	
Participant 01	Well, yes. There are a couple of things. First of all, I do spend a lot of time posting. It's not hours and hours, but I probably spend one or two hours a day posting or sharing posts because this is a political issue I think is really, really important. Number one, it's the time that I know maybe I could be doing other things. The other thing is I know that there's an element of danger because a number of academics from other universities have been sacked for supporting Palestine. So that's why I don't put my name. But I think if I am careful, the problems are outweighed by the positives. Sharing messages and sharing information in a sensible way has risks, but you know me a little bit, Marvin. I am not the quiet type. If I see something is wrong or something is good, if I can do anything to help anyone, I will. Life changes, and when I was your age, there was no social media. My mother	Codes: time tension; professional/reputational danger; benefits outweigh risks; risk-benefit reconciliation. Category: moral purpose versus risk.

Speaker	Dialogue	Memos / Notes
	said the biggest change in her life was the internet. It is a wonderful, wonderful tool. Look what we are doing now because of digital technology. So we have to be careful of absolutely everything, but if you were super, super, super careful and worried, then you wouldn't even leave the house. It's all about managing benefits and risks. Nothing is without risk.	
Interviewer	Even when you are aware of the risks, what keeps you using social media?	
Participant 01	Regarding Facebook, which I have an account but I don't use, I stopped using that because I saw bullying on it. My son was bullied on it. There was a lot of racism towards my son. People would post a picture of their house, their holiday, their next holiday, their new car. I'm not unhappy for them, but I don't really want people to see my new car or my new house or my new dog or my new boyfriend, not that I have one. I found that quite stressful because people tend to show you something and maybe it's not real. That is the big thing for me with Facebook. I don't like it. I really, really don't like it. But I am very, very passionate about some political issues, and Twitter or X and Instagram allow me to make some noise, create awareness, show my passion and show my concern for a very disadvantaged population. Where we are in 2026, when I see injustice, social media for me is a way to contribute to the debate, create awareness and chat with like-minded people. So yes, the risks are there and the risks are serious, but it is a channel that has opportunities for me to share messages about political issues.	Codes: Facebook withdrawal; social comparison; racism/bullying; awareness raising; like-minded community. Category: platform rejection and purposeful continuation.
Interviewer	How do you weigh the benefits of social media against the potential risks?	
Participant 01	It's really stuff I've already mentioned, but there are risks to everything. There are some people who are not politically interested, people who don't vote. I'm not one of these people. I think it goes back to my first degree in philosophy and a master's in political philosophy. It is something that I'm very, very interested in. When I started on social media, on Twitter, maybe I had three followers, then ten followers, then 100 followers, and I've got about 2,000 now. That is not two million or 200,000, but some people follow me and I follow people. It's not that it gives me a buzz, but it means that my message is getting out and I'm seeing similar posts regarding a particular issue that is very important to me.	Codes: political identity; audience growth; message circulation. Category: advocacy reward and public voice.
Interviewer	What do you tell yourself to justify continuing to use social media despite being aware of the risks?	
Participant 01	I say something very unusual, if you like. I believe that the right situation is eventually shown. If I don't have hope, there's no point spending two hours a night posting for Palestine. But I believe that this, just like apartheid in South Africa, ultimately will be recognised globally as wrong. That is the only thing that keeps me going. If I think about racial segregation in America and apartheid in South Africa, eventually the right and moral side won. That is what keeps me going. I'm always mindful not to disclose any personal information. I may mention Wales and Bahrain, but I wouldn't go into detail for fear of retaliation or trouble.	Codes: hope; historical justice analogy; non-disclosure; fear of retaliation. Category: moral rationalisation plus privacy boundary.
Interviewer	Do you take any steps to protect yourself from risk when using social media? Can you give me an example?	
Participant 01	I think, like I say, I don't use my name or family name. I don't post images or photographs of myself or my family. I don't post locations. Regarding social media, I wouldn't say these are just basic. I've just had so many accounts closed by sharing a post from Al Jazeera News. TikTok have shut me down twice, Instagram four times, LinkedIn once, and I'm just sharing that there has been a massacre of, say, 176 children. It's an incredibly powerful agenda. So the steps I take are not using my real name, not	Codes: pseudonym; no family images; no locations; account closure; private/public separation. Category: boundary management.

Speaker	Dialogue	Memos / Notes
	showing family, not showing locations and not giving people information that could connect my political views back to my private life.	
Interviewer	How do you manage your privacy or personal information on social media?	
Participant 01	I'm as vague as possible. So I lie about my date of birth. I removed 10 years. I don't use my name. I'm very vague.	Codes: vague identity; false DOB; minimal personal data. Category: privacy minimisation.
Interviewer	Have your social media habits changed over time because of the risks that you have already shared?	
Participant 01	I've kind of silently withdrawn from Facebook. One reason I still have it is that some old friends of mine from university are on Facebook and they live in Australia. I don't know their home addresses or telephone numbers. But I don't post at all and I don't follow my children either. Ultimately, I believe that awareness of problems, awareness of situations and spreading awareness is really important. As long as I don't give too much information away, where I work, who my husband is, then it is just managing risks like you would with any kind of risky activity. I don't know anybody who doesn't have a social media account. My mother is on Facebook all the bloody time and she is 84. My sons are on Snapchat. It is now part of life. Instead of things being on television, information is so quick. I saw the news about the Queen's husband on Instagram. It is so quick to see the Liverpool team sheet. I'm also a passionate Liverpool fan, and on Instagram you see players in training and chatting, and that gives me a great deal of pleasure. Of course, the other thing is that it's free, and I do these little speech marks because nothing is free. But at the point of contact, it's free, instant and interactive. It's just part of life. Even the university has apps. I compartmentalise my life. You have work Caroline and then you have Palestine Caroline. I want to do the right thing as much as I can. If I can do something good, I always, always will do good and not bad.	Codes: cautious adaptation; Facebook withdrawal; everyday embeddedness; compartmentalisation. Category: risk management without full withdrawal.
Interviewer	Thank you, ma'am. Thank you for your time.	
Participant 01	Okay. I want you to know, you must make notes as soon as we finish. I want you to think, because sometimes we went over the same things. You never asked me, 'Can you tell me a little bit more?' You have to be more in control and you have to listen to what the Participant 01 says and always know in your mind, what do I want? If she says something and you have covered something with an earlier question, have another question, have something in your pocket. I'll see you in a couple of weeks, yes? Give my regards to Mrs Gomes.	

Appendix C: Interview Question Matrix Summary

Research question	Interview question area	Analytical purpose
RQ1	Typical use, platform choice, risks and privacy/data experience	Establishes platform ecology and the contexts where risk is encountered.
RQ2	Conflict, continued use despite risk, benefit-risk weighing and justification	Explores ethical tension, privacy calculus and rationalisation.
RQ3	Protective steps, privacy management, behavioural change and Q11	Explores coping strategies, adaptation and platform/regulatory responsibility.

Appendix D: Cross-Case Theme Development Audit Trail

Phase	Action completed in the revised analysis	Outcome
Phase 1: Familiarisation	Read each P01-P06 analysis document and added reflective notes on striking points, tensions and surprises.	Participant-level understanding deepened before coding was interpreted.
Phase 2: Initial coding	Generated semantic and latent codes from each participant extract.	Codes captured benefits, risks, protections, rationalisations, adaptation and structural change.
Phase 2a: Master code lists	Added consolidated master code lists for each participant.	Dr. Caroline's feedback was addressed by making Phase 2 visible as a discrete output.
Phase 3: Searching for provisional groupings	Clustered codes into categories and participant-level provisional groupings.	Each case produced working analytical claims rather than topic summaries.
Phase 4: Preliminary review	Reviewed provisional groupings within each participant case only.	Groupings were retained as provisional and not treated as final themes.
Phase 5: Defining and naming	Defined provisional groupings with clear analytic meanings.	Labels were written as claims but remained open to revision after cross-case comparison.
Phase 6: Illustrative write-up	Wrote participant-level analytic accounts for P01-P06.	Participant cases were ready for cross-case comparison.
Cross-case synthesis	Compared all provisional groupings across P01-P06.	Six final cross-case themes were developed for the findings section.

References

1. Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K. and Wetzels, M. (2015) 'Unravelling the personalisation paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness', Journal of Retailing, 91(1), pp. 34-49. https://doi.org/10.1016/j.jretai.2014.09.005
2. Appel, H., Gerlach, A.L. and Crusius, J. (2022) 'Social comparison and envy on social media: A critical review', Current Opinion in Psychology, 45, 101302. https://doi.org/10.1016/j.copsyc.2022.101302
3. Athey, S., Catalini, C. and Tucker, C. (2017) 'The digital privacy paradox: Small money, small costs, small talk', Management Science, 63(12), pp. 4423-4438. https://doi.org/10.1287/mnsc.2016.2697
4. Ayorech, Z., Baldwin, J.R., Pingault, J.-B. et al. (2023) 'Gene-environment correlations and genetic confounding underlying the association between media use and mental health', Scientific Reports, 13, 1030. https://doi.org/10.1038/s41598-022-25374-0
5. Bartol, J. (2025) 'Disentangling the role of algorithm awareness and knowledge in digital inequalities: An empirical validation of an explanatory model', Information, Communication & Society, 28(4), pp. 557-574. https://doi.org/10.1080/1369118X.2024.2363896
6. Baruh, L., Secinti, E. and Cemalcilar, Z. (2017) 'Online privacy concerns and privacy management: A meta-analytical review', Journal of Communication, 67(1), pp. 26-53. https://doi.org/10.1111/jcom.12276
7. Berger, R. (2015) 'Now I see it, now I don't: Researcher's position and reflexivity in qualitative research', Qualitative Research, 15(2), pp. 219-234. https://doi.org/10.1177/1468794112468475
8. Boerman, S.C., Kruikemeier, S. and Zuiderveen Borgesius, F.J. (2017) 'Online behavioural advertising: A literature review and research agenda', Journal of Advertising, 46(3), pp. 363-376. https://doi.org/10.1080/00913367.2017.1339368
9. Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', Qualitative Research in Psychology, 3(2), pp. 77-101. https://doi.org/10.1191/1478088706qp063oa
10. Braun, V. and Clarke, V. (2019) 'Reflecting on reflexive thematic analysis', Qualitative Research in Sport, Exercise and Health, 11(4), pp. 589-597. https://doi.org/10.1080/2159676X.2019.1628806
11. Braun, V. and Clarke, V. (2022) Thematic Analysis: A Practical Guide. London: SAGE.
12. Brinkmann, S. and Kvale, S. (2015) InterViews: Learning the Craft of Qualitative Research Interviewing. 3rd edn. Thousand Oaks, CA: SAGE.
13. Bryman, A. and Bell, E. (2015) Business Research Methods. 4th edn. Oxford: Oxford University Press.
14. Burke, M. and Kraut, R.E. (2016) 'The relationship between Facebook use and well-being depends on communication type and tie strength', Journal of Computer-Mediated Communication, 21(4), pp. 265-281. https://doi.org/10.1111/jcc4.12162
15. Büchi, M. and Hargittai, E. (2022) 'A need for considering digital inequality when studying social media use and well-being', Social Media + Society, 8(1). https://doi.org/10.1177/20563051211069125
16. Clayton, K., Blair, S., Busam, J.A. et al. (2020) 'Real solutions for fake news? Measuring the effectiveness of general warnings and fact-check tags in reducing belief in false stories on social media', Political Behavior, 42, pp. 1073-1095. https://doi.org/10.1007/s11109-019-09533-0
17. Creswell, J.W. and Miller, D.L. (2000) 'Determining validity in qualitative inquiry', Theory Into Practice, 39(3), pp. 124-130. https://doi.org/10.1207/s15430421tip3903_2
18. Crotty, M. (1998) The Foundations of Social Research: Meaning and Perspective in the Research Process. London: SAGE.
19. Cunningham, S., Hudson, C.C. and Harkness, K. (2021) 'Social media and depression symptoms: A meta-analysis', Research on Child and Adolescent Psychopathology, 49, pp. 241-253. https://doi.org/10.1007/s10802-020-00715-7

20. De Wolf, R., Willaert, K. and Pierson, J. (2014) 'Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook', Computers in Human Behavior, 35, pp. 444-454. https://doi.org/10.1016/j.chb.2014.03.010
21. Dhir, A., Yossatorn, Y., Kaur, P. and Chen, S. (2018) 'Online social media fatigue and psychological wellbeing: A study of compulsive use, fear of missing out, fatigue, anxiety and depression', International Journal of Information Management, 40, pp. 141-152. https://doi.org/10.1016/j.ijinfomgt.2018.01.012
22. Dienlin, T. and Trepte, S. (2015) 'Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviours', European Journal of Social Psychology, 45(3), pp. 285-297. https://doi.org/10.1002/ejsp.2049
23. Dienlin, T., Masur, P.K. and Trepte, S. (2023) 'A longitudinal analysis of the privacy paradox', New Media & Society. https://doi.org/10.1177/14614448211016316
24. Dinev, T. and Hart, P. (2006) 'An extended privacy calculus model for e-commerce transactions', Information Systems Research, 17(1), pp. 61-80. https://doi.org/10.1287/isre.1060.0080
25. Ellison, N.B., Steinfield, C. and Lampe, C. (2007) 'The benefits of Facebook friends: Social capital and college students' use of online social network sites', Journal of Computer-Mediated Communication, 12(4), pp. 1143-1168. https://doi.org/10.1111/j.1083-6101.2007.00367.x
26. Ellison, N.B., Vitak, J., Gray, R. and Lampe, C. (2014) 'Cultivating social resources on social network sites: Facebook relationship maintenance behaviours and their role in social capital processes', Journal of Computer-Mediated Communication, 19(4), pp. 855-870. https://doi.org/10.1111/jcc4.12078
27. Fardouly, J., Diedrichs, P.C., Vartanian, L.R. and Halliwell, E. (2015) 'Social comparisons on social media: The impact of Facebook on young women's body image concerns and mood', Body Image, 13, pp. 38-45. https://doi.org/10.1016/j.bodyim.2014.12.002
28. Finlay, L. (2002) 'Negotiating the swamp: The opportunity and challenge of reflexivity in research practice', Qualitative Research, 2(2), pp. 209-230. https://doi.org/10.1177/146879410200200205
29. Grinberg, N., Joseph, K., Friedland, L., Swire-Thompson, B. and Lazer, D. (2019) 'Fake news on Twitter during the 2016 U.S. presidential election', Science, 363(6425), pp. 374-378. https://doi.org/10.1126/science.aau2706
30. Guess, A., Nagler, J. and Tucker, J. (2019) 'Less than you think: Prevalence and predictors of fake news dissemination on Facebook', Science Advances, 5(1), eaau4586. https://doi.org/10.1126/sciadv.aau4586
31. Hargittai, E. and Marwick, A. (2016) 'What can I really do? Explaining the privacy paradox with online apathy', International Journal of Communication, 10, pp. 3737-3757.
32. Hunt, M.G., Marx, R., Lipson, C. and Young, J. (2018) 'No more FOMO: Limiting social media decreases loneliness and depression', Journal of Social and Clinical Psychology, 37(10), pp. 751-768. https://doi.org/10.1521/jscp.2018.37.10.751
33. Joinson, A.N. (2008) 'Looking at, looking up or keeping up with people? Motives and use of Facebook', Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1027-1036. https://doi.org/10.1145/1357054.1357213
34. Keles, B., McCrae, N. and Grealish, A. (2020) 'A systematic review: The influence of social media on depression, anxiety and psychological distress in adolescents', International Journal of Adolescence and Youth, 25(1), pp. 79-93. https://doi.org/10.1080/02673843.2019.1590851
35. Kim, Y. (2011) 'The pilot study in qualitative inquiry: Identifying issues and learning lessons for culturally competent research', Qualitative Social Work, 10(2), pp. 190-206. https://doi.org/10.1177/1473325010362001
36. King, N. and Horrocks, C. (2010) Interviews in Qualitative Research. London: SAGE.
37. Krasnova, H., Spiekermann, S., Koroleva, K. and Hildebrand, T. (2010) 'Online social networks: Why we disclose', Journal of Information Technology, 25(2), pp. 109-125. https://doi.org/10.1057/jit.2010.6
38. Kross, E., Verduyn, P., Demiralp, E. et al. (2013) 'Facebook use predicts declines in subjective well-being in young adults', PLoS ONE, 8(8), e69841. https://doi.org/10.1371/journal.pone.0069841

39. Lin, L.Y., Sidani, J.E., Shensa, A. et al. (2016) 'Association between social media use and depression among U.S. young adults', Depression and Anxiety, 33(4), pp. 323-331. https://doi.org/10.1002/da.22466
40. Lincoln, Y.S. and Guba, E.G. (1985) Naturalistic Inquiry. Beverly Hills, CA: SAGE.
41. Litt, E. (2013) 'Understanding social network site users' privacy tool use', Computers in Human Behavior, 29(4), pp. 1649-1656. https://doi.org/10.1016/j.chb.2013.01.049
42. Liyanaarachchi, G., Mifsud, M. and Viglia, G. (2024) 'Virtual influencers and data privacy: Introducing the multi-privacy paradox', Journal of Business Research, 176, 114584. https://doi.org/10.1016/j.jbusres.2024.114584
43. Lu, H., Wei, A. and Li, X. (2025) 'Understanding the privacy disclosure behavior and privacy concerns on short-form video platforms: An empirical investigation', Frontiers in Psychology, 16, 1535533. https://doi.org/10.3389/fpsyg.2025.1535533
44. Lup, K., Trub, L. and Rosenthal, L. (2015) 'Instagram #Instasad?: Exploring associations among Instagram use, depressive symptoms, negative social comparison, and strangers followed', Cyberpsychology, Behavior, and Social Networking, 18(5), pp. 247-252. https://doi.org/10.1089/cyber.2014.0560
45. Maier, C., Laumer, S., Eckhardt, A. and Weitzel, T. (2015) 'Giving too much social support: Social overload on social networking sites', European Journal of Information Systems, 24(5), pp. 447-464. https://doi.org/10.1057/ejis.2014.3
46. Meier, Y. and Krämer, N.C. (2024) 'The privacy calculus revisited: An empirical investigation of online privacy decisions on between- and within-person levels', Communication Research. https://doi.org/10.1177/00936502221102101
47. Min, J. and Kim, B. (2015) 'How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost', Journal of the Association for Information Science and Technology, 66(4), pp. 839-857. https://doi.org/10.1002/asi.23206
48. Nguyen, T.T., Tran, V.T.T. and Hoang, M.T.T. (2024) 'How peer privacy concerns affect active and passive uses of social networking sites: A dual peer privacy calculus model', Social Science Computer Review, 42(6). https://doi.org/10.1177/08944393231224539
49. Nissenbaum, H. (2010) Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA: Stanford University Press.
50. Norberg, P.A., Horne, D.R. and Horne, D.A. (2007) 'The privacy paradox: Personal information disclosure intentions versus behaviours', Journal of Consumer Affairs, 41(1), pp. 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x
51. Oeldorf-Hirsch, A. and Neubaum, G. (2023) 'Attitudinal and behavioral correlates of algorithmic awareness among German and U.S. social media users', Journal of Computer-Mediated Communication, 28(5), zmad035. https://doi.org/10.1093/jcmc/zmad035
52. Orben, A. and Przybylski, A.K. (2019) 'The association between adolescent well-being and digital technology use', Nature Human Behaviour, 3, pp. 173-182. https://doi.org/10.1038/s41562-018-0506-1
53. Parry, D.A., Davidson, B.I., Sewall, C.J.R., Fisher, J.T., Mieczkowski, H. and Quintana, D.S. (2021) 'A systematic review and meta-analysis of discrepancies between logged and self-reported digital media use', Nature Human Behaviour, 5, pp. 1535-1547. https://doi.org/10.1038/s41562-021-01117-5
54. Patton, M.Q. (2015) Qualitative Research & Evaluation Methods. 4th edn. Thousand Oaks, CA: SAGE.
55. Pennycook, G. and Rand, D.G. (2019) 'Fighting misinformation on social media using crowdsourced judgments of news source quality', Proceedings of the National Academy of Sciences, 116(7), pp. 2521-2526. https://doi.org/10.1073/pnas.1806781116
56. Primack, B.A., Shensa, A., Sidani, J.E. et al. (2017) 'Social media use and perceived social isolation among young adults in the U.S.', American Journal of Preventive Medicine, 53(1), pp. 1-8. https://doi.org/10.1016/j.amepre.2017.01.010

57. Quan-Haase, A. and Young, A.L. (2010) 'Uses and gratifications of social media: A comparison of Facebook and instant messaging', Bulletin of Science, Technology & Society, 30(5), pp. 350-361. https://doi.org/10.1177/0270467610380009
58. Ravindran, T., Kuan, A.C.Y. and Lian, D.G.H. (2014) 'Antecedents and effects of social network fatigue', Journal of the Association for Information Science and Technology, 65(11), pp. 2306-2320. https://doi.org/10.1002/asi.23122
59. Roberts, J.A., Young, P.D. and David, M.E. (2026) 'The epidemic of loneliness: A 9-year longitudinal study of the impact of passive and active social media use on loneliness', Personality and Social Psychology Bulletin. https://doi.org/10.1177/01461672241295870
60. Sametoğlu, S., Pelt, D.H.M. and Bartels, M. (2025) 'The association between frequency of social media use, wellbeing, and depressive symptoms: Disentangling genetic and environmental factors', Behavior Genetics, 55, pp. 255-269. https://doi.org/10.1007/s10519-025-10224-2
61. Shakya, H.B. and Christakis, N.A. (2017) 'Association of Facebook use with compromised well-being: A longitudinal study', American Journal of Epidemiology, 185(3), pp. 203-211. https://doi.org/10.1093/aje/kww189
62. Smit, E.G., Van Noort, G. and Voorveld, H.A.M. (2014) 'Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe', Computers in Human Behavior, 32, pp. 15-22. https://doi.org/10.1016/j.chb.2013.11.008
63. Taddicken, M. (2014) 'The privacy paradox in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure', Journal of Computer-Mediated Communication, 19(2), pp. 248-273. https://doi.org/10.1111/jcc4.12052
64. Tandoc, E.C., Ferrucci, P. and Duffy, M. (2015) 'Facebook use, envy, and depression among college students: Is Facebooking depressing?', Computers in Human Behavior, 43, pp. 139-146. https://doi.org/10.1016/j.chb.2014.10.053
65. Tracy, S.J. (2010) 'Qualitative quality: Eight "big-tent" criteria for excellent qualitative research', Qualitative Inquiry, 16(10), pp. 837-851. https://doi.org/10.1177/1077800410383121
66. Turel, O. and Serenko, A. (2012) 'The benefits and dangers of enjoyment with social networking websites', European Journal of Information Systems, 21(5), pp. 512-528. https://doi.org/10.1057/ejis.2012.1
67. Valkenburg, P.M. (2022) 'Social media use and well-being: What we know and what we need to know', Current Opinion in Psychology, 45, 101294. https://doi.org/10.1016/j.copsyc.2021.12.006
68. Valkenburg, P.M., Beyens, I., Meier, A. and Vanden Abeele, M.M.P. (2022) 'Advancing our understanding of the associations between social media use and well-being', Current Opinion in Psychology, 47, 101357. https://doi.org/10.1016/j.copsyc.2022.101357
69. Valkenburg, P.M., Meier, A. and Beyens, I. (2022) 'Social media use and its impact on adolescent mental health: An umbrella review of the evidence', Current Opinion in Psychology, 44, pp. 58-68. https://doi.org/10.1016/j.copsyc.2021.08.017
70. van Teijlingen, E.R. and Hundley, V. (2001) 'The importance of pilot studies', Social Research Update, 35, pp. 1-4.
71. Verduyn, P., Lee, D.S., Park, J. et al. (2015) 'Passive Facebook usage undermines affective well-being: Experimental and longitudinal evidence', Journal of Experimental Psychology: General, 144(2), pp. 480-488. https://doi.org/10.1037/xge0000057
72. Verduyn, P., Ybarra, O., Résibois, M., Jonides, J. and Kross, E. (2017) 'Do social network sites enhance or undermine subjective well-being? A critical review', Social Issues and Policy Review, 11(1), pp. 274-302. https://doi.org/10.1111/sipr.12033
73. Vitak, J. (2012) 'The impact of context collapse and privacy on social network site disclosures', Journal of Broadcasting & Electronic Media, 56(4), pp. 451-470. https://doi.org/10.1080/08838151.2012.732140
74. Vogel, E.A., Rose, J.P., Roberts, L.R. and Eckles, K. (2014) 'Social comparison, social media, and self-esteem', Psychology of Popular Media Culture, 3(4), pp. 206-222. https://doi.org/10.1037/ppm0000047

75. Vosoughi, S., Roy, D. and Aral, S. (2018) 'The spread of true and false news online', Science, 359(6380), pp. 1146-1151. https://doi.org/10.1126/science.aap9559
76. Vuorre, M. and Przybylski, A.K. (2024) 'Global well-being and mental health in the Internet age', Clinical Psychological Science. https://doi.org/10.1177/21677026231207791
77. Whiting, A. and Williams, D. (2013) 'Why people use social media: A uses and gratifications approach', Qualitative Market Research, 16(4), pp. 362-369. https://doi.org/10.1108/QMR-06-2013-0041
78. Xu, H., Dinev, T., Smith, H.J. and Hart, P. (2011) 'Information privacy concerns: Linking individual perceptions with institutional privacy assurances', Journal of the Association for Information Systems, 12(12), pp. 798-824. https://doi.org/10.17705/1jais.00281
79. Young, A.L. and Quan-Haase, A. (2013) 'Privacy protection strategies on Facebook: The Internet privacy paradox revisited', Information, Communication & Society, 16(4), pp. 479-500. https://doi.org/10.1080/1369118X.2013.777757